2ND Edition

Network Fundamentals

By: Basem Hamed

To

The Girl that always supports me, Loving You My Darling

Basem

About Author: -

Basem Hamed is a network and security engineer. He has been building his knowledge and experience for more than 11 years. He is interested in information security and data center fields. Basem worked at many companies in different positions, but he is passionate about instructing.

He has Authored books in Microsoft "Active Directory and Infrastructure 2008 "and in Cisco "CCNA Practical Books"

Please contact me if you need these books.

Delivered Courses if you Need them: -

CCNA
CCNP ENCOR
CCNP ENARSI
CCNP SCOR
MSCA 2012-2016
Azure
Security+

Contacts: -

basem.cloud@gmail.com

/basemhamed.13

in/basemhamed

01001582348

Network Fundamental

is considered as the Basics for anyone wants to know what the Network is. This Book Provides an overview of basic networking concepts, including network architecture, devices, design and components. The Book covers media types and standards and how data is encoded and transmitted.

Speaking in-depth about application coverage includes email, the domain name system, the World Wide Web and multimedia (including voice over IP, Internet radio video on demand, video conferencing and streaming media). Each chapter follows a consistent approach: the Book presents key principles and then illustrates them utilizing real-world example networks that run through the Internet, IP Addresses, Cables, Network Models and Network Devices.

1st Edition, 2015
2nd Edition 2023

ملاحظات: -

الكتاب صدقه جاريه علي روح والدي ووالدتي وحمايا – نسألكم الدعاء ليهم ولينا

الشرح اللي هنا مركز على الجزء النظري الخاص بأساسيات الشبكات – اللي الناس تتلخبط فيها او الناس عايزة تبدأ في المجال وفي مصطلحات ناقصاها او لسه مش عارفه أنواع الكابلات او تحل مسائل الـ Subnetting او حتي كمان بتنسي الـ OSI Model

لو في اي حاجة مش واضحه مع اي حد وعايز يستفسر عن اي حاجه يتصل عليا او يبعتلي في اي وقت وان شاء الله انا هرد عليه

حاولت اني ابسط المعلومة علي قد ما أقدر واوصلها بكل الأساليب البسيطة الممكنة

بالتوفيق للجميع

باسم حامد

Content: -

Network Topology

قبل البداية في الحديث عن أي شيء – يجب ان نتعرف سويا علي معني ومفهوم Network

هو توصيل الأجهزة مع بعضها باستخدام Centralize Device لضمان وجود Connectionبين الأجهزة وبعضها

الغرض منها هو عمل Sharing of Recourses

- Hardware – File Server
- Software – any Application
- Service – Internet or Printer and etc. ...
- Simple Data



Network Topology

مصطلح يندرج تحته مفهوم طريقة توصيل الأجهزة مع بعضها وايضا طريقة الــ Connection التي تحدث بين الأجهزة وبعضها

لها نوعان :-

Virtual or Logical Topology, Physical Topology

Virtual Topology

معناها كيف يتم نقل الداتا بين الأجهزة وبعضها - How Devises are Communicate ؟

مثل Bus Topology and Ring Topology with Token -:

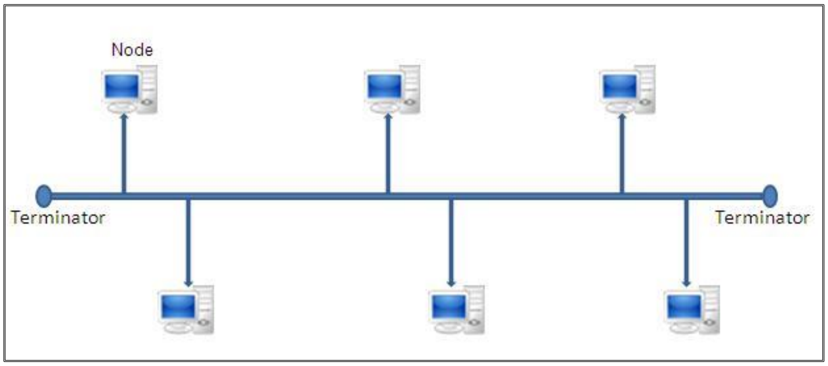
Physical Topology

معناها كيف يتم توصيل الأجهزة مع بعضها البعض وما هو شكل الداتا وطريقه نقلها -- How Devises are Connected ؟

مثل Star Topology and Ring Topology with MAU

لنتحدث عن كل منهم بالتفصيل

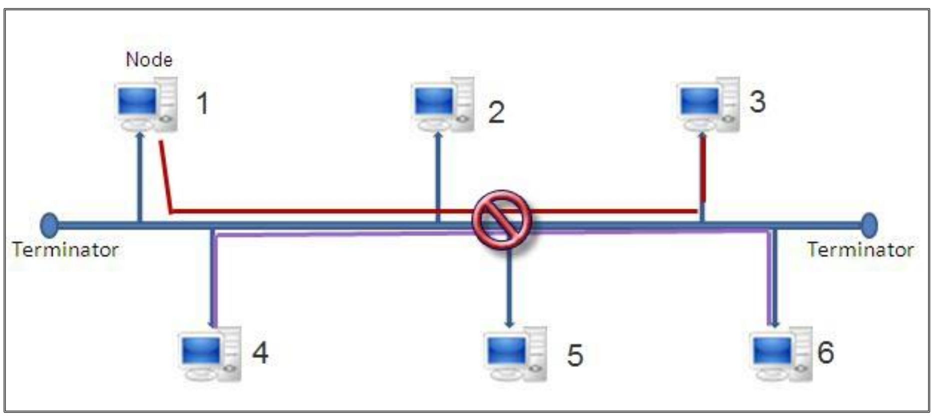
1- Bus Topology :-



مجموعة من الأجهزة يتم توصيلها علي Line واحد كما هو موضح في الشكل .
وكما تم التوضيح من قبل أن هذا النوع هو أول انواع الـ Virtual Topology – أي انه لا يوجد في الـ Real Life توصيل يتم كهذا ولكن !!
كان هذه هي بداية التوصيل من قبل .
في نهاية الـ Line يوجد Device يسمي Terminator
هذا النوع كان أرخص انواع التوصيل وكان بدائي جدا في التوصيل

كان هناك عيوب كثيرة جدا لهذا التصميم من أهم عيوبها هو الــ :-

Collision



لو Source PC1 يقوم بإرسال Data او Access على أي service على PC3 Destination وفي نفس الوقت يقوم جهاز آخر مثل PC6 يقوم بعمل Access على PC4
فإن الـ Data المرسلة كل الأجهزة ستقوم باستلامها لأنها مرسلة Broadcast

مصطلح Broadcast معناه :-
إن جهاز معين او بيانات معينة محتاج إنك ترسلها لشخص واحد للأسف بتوصل لكل الناس اللي موجودة عندك – زي اللي موجودة كدا على الـ WhatsApp اللي نستخدمه One to All Traffic

نفس الفكرة مع الأجهزة

في الحالة الأولي PC1 مع PC3 ولكن باقي الأجهزة حدث انها استلمت داتا او استلمت طلب ليس لها فستقوم بعمل Drop له ولكن حدث Loop في الشبكة حتى تصل الي الـ Destination المطلوب

بالإضافة الي الـ Loop مع وجود جهازين ايضا يقومون بالاتصال مع بعض فسيحدث Collision أي تصادم في نقل الData بين الأجهزة وبعضها وسيحدث Drop لكل الـ Packets المرسلة

للتغلب علي مشكلة الـ Collision :-

CSMA / CD

Carrier Sense Multiple Access / Collision Detection

تحدث فقط في شبكات الـ Wired

أي ان اي جهاز يقوم بإرسال Data لأي جهاز آخر يقوم بعمل Sense للـ Carrier او الحامل الذي يقوم بنقل الداتا حتي يتأكد هل هناك جهاز أخر يقوم بالإرسال في نفس الوقت أم لا Multiple Access

حتي يحدث Detect للـ Collision الذي قد يحدث بين الأجهزة

ولكن إذا حدث ايضا ارسال في نفس الوقت سيحدث Collision و Drop للـ Packet المرسلة

(تقلل من حدوث التصادم وليس منعه نهائيا)

هناك مصطلح آخر يسمي CSMA / CA

Carrier Sense Multiple Access / Collision Avoidance

اي تجنب حدوث الـ Collision من الاساس وهي تحدث في شبكات الـ Wireless لأنه في هذا النوع من الـ Connection لا يجب ان يحدث Collision من الأساس

Jamming of Signal

تحدث بمجرد حدوث الCollision – وتقوم بإعطاء كل الأجهزة Random of Time وبيكون في الغالب بالميللي ثانية وقت عشوائي لكل الأجهزة لغرض انه بعد انتهاء هذا الوقت يقوم الجهاز بعمل إرسال للـ Data كما يريد لتجنب حدوث الـ Collision بين الأجهزة



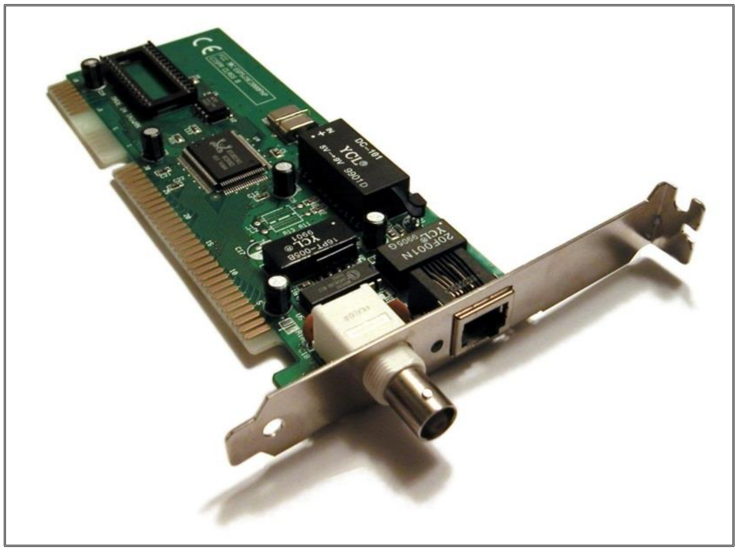
وظيفة الـ Terminator

يقوم بامتصاص الإشارة الموجودة في الـ Carrier او الـ Line او الـ Cable بعد ان يتم ارسالها Broadcast لكل الأجهزة -- حتي لا يتم تكرارها مره أخري في الـ Network

لتجنب حدوث Loop بعد الـ Loop الأساسي الحادث بسبب الـ Broadcast

كان يستخدم في هذه الـ Topology نوع من انواع الـ Cables يسمي Co-Axil Cable – مثل المستخدم في اجهزه الدش – وسيكون هناك Document منفصلة تتحدث عن ال Cables

وأيضا كان يستخدم Network Interface Card يستخدم في توصيله الـ Co-Axil سنتكلم عنه بالتفصيل في شابتر الـ Cables



في بداية الـ Topology كان يستخدم الـ Terminator ثم بعد ذلك ظهر الـ Hub -- وكلاهما كان يدعم الـ Co-Axil Cable وكلاهما كان يحدث بسببهم Collision & Broadcast لأن لا يوجد من ضمن الـ Internal Component الخاصة بهم Processor

سنحدث عنهم في الـ Document القادم

Broadcast Domain

هو عدد رسائل الـ Broadcast اللي ممكن انه يتم ارسالها من نقطة لآخري

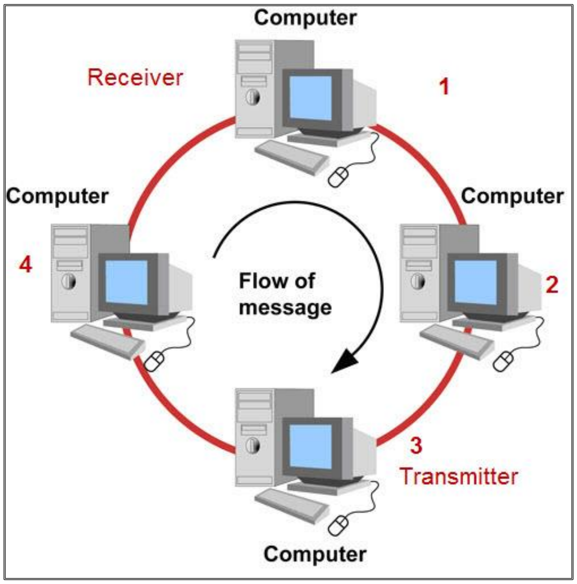
Collison Domain

عدد التصادمات اللي ممكن حدوثها

Device	Broadcast Domain	Collision Domain
Hub	1	1
Switch	1	Based on Number of connected Devices Per Interface
Router	Based on Number of connected Devices Per Interface	Based on Number of connected Devices Per Interface

Ring Topology -2

I – Ring Topology Using Token



تاني نوع من انواع الـ Virtual or Logical Topology - حينما يقوم PC3 Transmitter بإرسال Data الي PC1 Receiver

سيتم انشاء ما يسمي الـ Token بواسطة الـ Transmitter

الـ Token

Virtual Thing تحتوي علي الـ Dataالمرسلة بالإضافة الي الـ Destination MAC Address & IP

PC3 سيتأكد ان الـ Token Free أي لا يقوم أي PC آخر بإرسال Data

سيقوم بعمل Load للـ Data علي الـ Token -- وعمل أيضا Load للـ Source and Destination Address IP

يتم إرسال الـ Token بــ Broadcast الي كل الأجهزة المتصلة مع بعض في الـ Network

وظيفة عمل الـ Receiver عند استلام الـ Data

1- هيعمل Check ان هو الـ Address المطلوب
2- هياخد الـ Data المرسلة Copy وليس Cut
3- هيعمل Repeat للـ Data , إعادة إرسال او إعادة تقوية للإشارة المرسلة
4- يتم وضع Mark انه تم استلام الـ Data بنجاح

كما وضحنا انه سيتم إرسالها Broadcast – فإن الـ Data سيتم وصولها إلي الـ Transmitter مرة إخري

بعد وصول الـ Token مرة إخري إلي الـ Transmitter

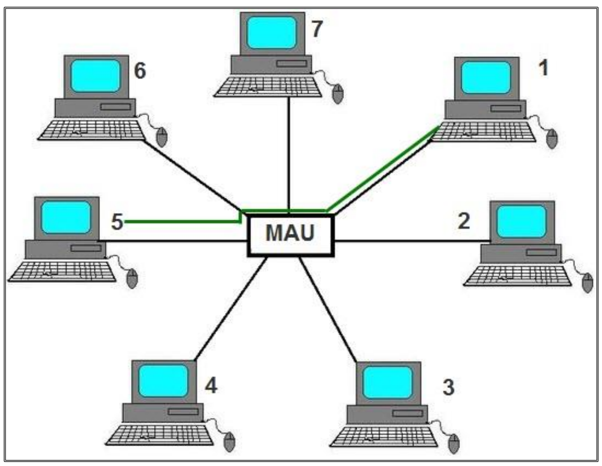
1- سيقوم بالتأكد انه تم إستلام الـ Data عن طريق الـ Mark الذي قام الـ Receiver بوضعها
2- سيقوم بعمل Delete للـ Data من الـ Token
3- ستصبح الـ Token خالية Empty لأي جهاز آخر ليستخدمها

وهنلاحظ هنا ان مفيش Collision هيحصل علشان هيا Token واحدة بس اللي بيتعمل ليها Create

II – Ring Topology Using MAU

أول انواع الـ Physical Topologies - أي ان هناك فعليا Devise يتم من خلاله توصيل الأجهزة مع بعضها البعض Centralize Device

الـ Media Access Unit MAU --- هو المسئول عن انشاء الـ Token وإرسالها الي الـ Receiver المطلوب



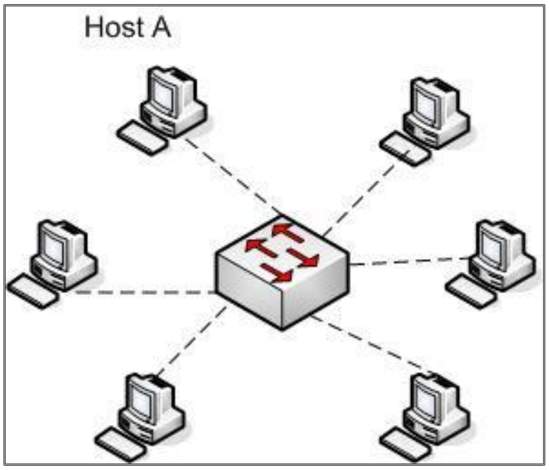
1- PC1 سيقوم بإرسال Data الي PC5 من خلال الـ MAU
2- سيتم إرسال الـ Data بـ Broadcast الي كل الأجهزة المتصلة مع بعضها من خلاص الـ MAU
3- مثلا PC2 سيقوم بعمل Check علي الـ Data المرسلة || هل هو الـ Receiver المطلوب ام لا
4- إذا كان ليس هو المطلوب سيقوم بإرسال الـ Data مرة ثانية الي الـ MAU – وسيحدث هذا مع كل الأجهزة حتي يصل الي الـ Receiver المطلوب
5- حتي يتم إرسالها الي PC5 وهو الجهاز المطلوب .
6- سيقوم بعمل Copy and Mark للـ Data المرسلة
7- بعد ذلك سيقوم بعمل Release or Delete للـ Data من الـ Token وارسالها Empty الي الـ MAU

في الـ Ring Topology بأنواعها لا يحدث Collision

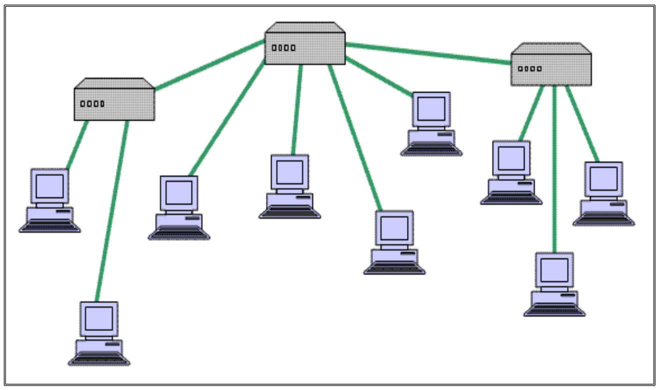
لأن الـ Data يتم ارسالها واستقابلها من خلال الـ Token وطالما الـ Token مشغول فلن يستطيع اي جهاز ارسال Data لجهاز آخر

ولكن المشكلة الفعليه كانت في الـ Broadcast

Stat Topology -4

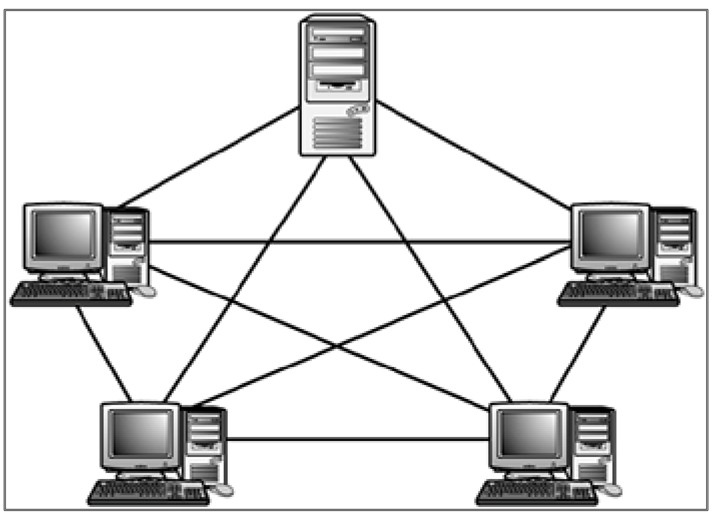


أفضل أنواع الـ Topology والتي يتم استخدامها حاليا
كان الـ Devises المستخدمة بدأت في التطور من الـ Hub → Repeater → Bridge → Switch
وهذة سيكون محور حديثنا في الـ Document القادمة
ومراحل تطورها وما هي الأجهزة المستخدمه حاليا – Network Devises
وكانت بتعتمد علي الـ Device المركزي اللي متوصل عليه كل الـ PC's

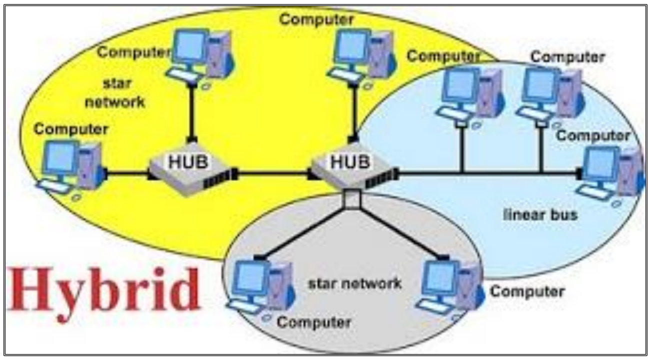


أكتر من Star Topology ← Tree Topology

Mesh Topology -5



الغرض منها اني أضمن الـ Stability والـ
Redundancy في توصيل الأجهزة ونقل الـ Data بين
الأجهزه وهي بالطبع Logical Topology
توضيح علي هذه الصورة – اذا أردت فعليا توصيلهم علي
هذة الشاكلة ستقوم بإضافة NIC 4 لكل جهاز
ولكنها تستخدم للتوصيل بين الـ Switches



Hybrid Topology -6

توصيل أكتر من نوع من أنواع الـ Topologies مع بعضهم

كما في الـ Diagram

	Bus Topology	Ring Topology	Star Topology
Speed	10 M.Bit/S	45 M.Bit/S	100 M.Bit/S
Device	Terminator or Hub	Token or MAU	Hub or Switch
Cables	Co-Axil or UTP	UTP	UTP

Communication Type	Description
Simple Duplex	في النوع دا اما الـ Cable بيعت داتا او يستقبل داتا "زي الـ Cable بتاع التليفزيون"
Half Duplex	بيعت داتا وبستقبل داتا بس مش في نفس الوقت " زي اللاسلكي بتاع الشرطة" وزي الـ Bluetooth والـ Wireless
Full Duplex	ببعت وبستقبل في نفس الوقت زي الـ Cables اللي بنستخدمها بين الأجهزة

Networking Type

LAN → Local Area Network

مجموعة من الأجهزة Connected مع بعض in Small Area أو in the Same Location
مثل :-

- Ethernet 10Mb/S
- Fast Ethernet 100 Mb/S
- Giga Ethernet 1000 Mb/S
- 10 Giga Ethernet 10Gb/S

WAN → Wide Area Network

Used to connect LANs together .Typically, WANs are used when the LANs that must be connected are separated by a large distance

MAN → Metropolitan Area Network

Hybrid between a LAN and a WAN

PAN → Personal Area Network

Like Bluetooth

SAN → Storage Area Networks

Between Storage Devices and File Servers

يتم انشائها وتوصيلها بين أجهزت التخزين والسيرفرات وفي الغالب يتم استخدامها في الـ Data Center

Advantage:-

- Performance is fast.
- Availability is high because of the redundancy features available.
- Distances can span up to 10 kilometers.
- Management is easy because of the centralization of data resources.

Disadvantage of SANs is their Cost.

This Page Intentionally* Left *Blank

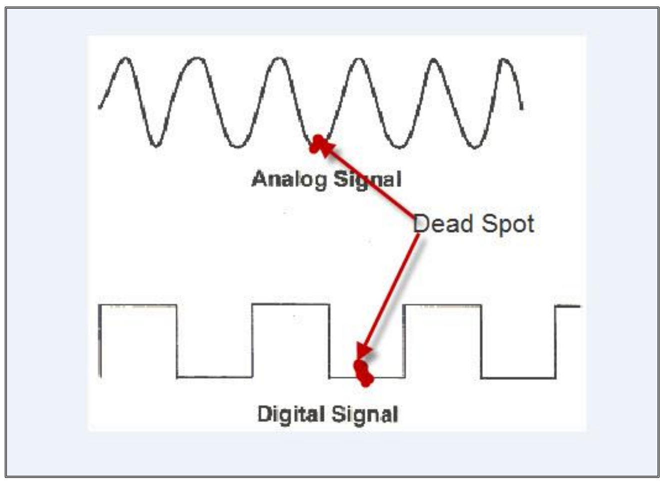
Network Devices

سنتكلم عن بعض الـ Devices المستخدمة في عالم الـ Network ولكن بشيء من التفصيل نظرا لأهميتهم فيما بعد – أيا كان تخصصك في مجال الـ Network

وسنحاول في حديثنا عن الـ Devices ان نقوم بتوضيحها نظرا لتطورها التكنولوجي بداية من الأنواع الأولي حتي ما آلت اليه التكنولوجيا في يومنا الحالي

1- Terminators
تكلمنا عنه في الـ Document السابق وقولنا انه يقوم بامتصاص الـ Signal حتي لا يحدث Loop أكثر من مرة في الشبكة وكان يستخدم مع الـ Bus Topology

2- Repeater
يقوم بعمل Re-generate للـ Signal



إذا تم نقل الـ Data الي مسافات طويله يحدث لها Drop وتشويش Noising، لذا يجب من وجود Device يقوم بعمل Re-generate للإشارة Signal التي تحمل ال Data

وايضا ينصح بأنه يجب الا يزيد طول الـ Cable الذي يتم توصيله بين الـ PC والـ Device المسئول عن الـ Internet Service عن 100Meter وممكن تختلف علي حسب نوع الكابل المستخدم في التوصيل زي ما هيتم توضيحه في الجزء الخاص بالـ Cables, حتي لا يحدث Drop للـ Signal ويكون الـ Internetبطئ -- يستخدم الـ Repeater مع الـ Digital Signal



أما مع الـ Analog Signal يستخدم جهاز يسمي الـ Amplifier ولكن وظيفته هو تضخيم الإشارة وليس Re-Generate

- يقوم بإرسال الـ Data إلي كل الأجهزة المتصلة أي Broadcast

أنواع الـ Repeater

- Wireless Repeater
- Wired Repeater (Booster _ Extender)

في بعض أنواع الـ Access Point بيكون فيها Bridge و Repeater للـ SSID الموجودة فيها وبتفرق علي حسب استخداماتك او المطلوب منها ايه



3- Connector

نفس وظيفة عمل الـ Repeater وهي Re-Generate ولكن الاختلاف هنا ان الـ Connector يقوم بتوصيل One Cable فقط – اي جهاز كومبيوتر
اما في الـ Repeater يمكننا توصيل أكتر من جهاز كومبيوتر علي نفس الـ Device

يمكننا ان نعتبر:-

Repeater → Multi port Connector



4- Hub

كانت بداية ظهور الـ Multi-Port Devices هي الـ Hub
يستخدم الـ Hub كمشترك يقوم بتجميع اكتر من جهاز كومبيوتر في مكان واحد لعمل LAN داخلية

من أهم عيوبه :-

- انه كان يقوم بعمل Share للـ Bandwidth (السرعة المستخدمة في نقل الـ Data)
بمعني انه إذا كان لديك سرعه 100 M.bit/S وتوجد اجهزة تتصل مع بعض سيقوم بتقسيم السرعة علي عدد الأجهزة المتصلة به

- أيضا انه كان يقوم بإرسال كل الـ Data المرسلة Broadcast لكل الأجهزة المتصلة معه في الشبكه – فيحدث Loop في الشبكة – لأنه لا يملك من ضمن الـ Component الخاصة به Processor ليقوم بتخزين الـ MAC Address الخاص بالأجهزة المتصلة معه - وذلك ينتج عنه حدوث Collision .

Hub → Multi-port Repeater

Type of Hub

1- Active Hub	➢ Support CSMA/CD ➢ Re-Generate of Data and Sending it ➢ Using only UTP Cables
2- Passive Hub	➢ Sending Data Only ➢ Using only UTP Cables
3- Hybrid Hub	➢ Support CSMA/CD ➢ Re-Generate of Data and Sending it ➢ Using Co-Axil and UTP Cables
4- Intelligent Hub	➢ Support IGMP (internet Group Management Protocol) ➢ Using 10 Base.T Co-Axil



5- Bridge

بداية ظهور الـ Smart Devices التي تستطيع ان تتعامل مع الـ MAC Address للتغلب علي مشكلة الـ Collision التي تحدث
يقوم بإرسال الـ Data للأجهزة Unicast وليست Broadcast

Bridge Type

1- Transparent Bridge	➢ Not Supporting CRC Cyclic Redundancy Check
2- Mixed Media Bridge	➢ Support CRC | Error Detection only
3- Local Bridge	➢ Between Rooms in the Same Building الـ Hardware الخاص به غالي
4- Remote Bridge	➢ Between More than One Building

سيتم الحديث عن الـ CRC بالتفصيل في الـ Document القادم



6- Switch

- من اهم الـ Devices التي تتعامل معها في شبكتك او شركتك
- و هذا هو النوع المستخدم حاليا في الشركات لتوصيل الأجهزة مع بعضها البعض حتى نقوم بعمل Sharing of Resources الموجودة
- Switch is a Smart Device لأنه يملك في الـ Component الخاصة به Processor يقوم بتخزين الـ MAC Address الخاص بالأجهزة حتي يتغلب علي مشكله الـ Broadcast ومشكله الـ Collision التي تحدث
- لأنه يقوم بإرسال الـ Data – Unicast أي محددة الي وجهتها المقصودة , و لا يتم إرسالها الي كل الأجهزة
- تغلب علي كل العيوب الموجوده في الـ Hub
- لا يقوم بعمل Share للـ Bandwidth المستخدمة

Unicast ➔ One to One

- أغلبية الـ Switches التي نستخدمها في البيوت يكون نوعها Un-Managed أو End Users ولا يمكننا عمل اي تعديلات عليها او عمل Configuration

Just Only Connecting PC's

- ولكن هناك شركات تقوم بتصنيع Switches يمكنك عمل اي Configuration تريدها عليها مثل CISCO and Juniper و هناك كورسات و Material حتي تستطيع ان تتعامل معها - السوتشات من طبيعة شغلها انها بتكون Plug and Play يعني مش محتاج Configuration علشان السويتش يشتغل بمجرد توصيله تقدر تستفيد بالخدمة المصنع لأجلها و هي Connect all Devices Together

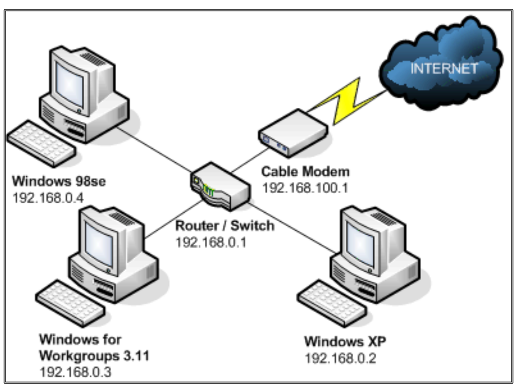
Switching Mode

❖ Cut Throw	- يقوم بإرسال الـ Data الي الـ Destination المطلوب دون إجراء اي تعديل فيها او تصحيح
❖ Store and Forward	- يقوم بتخزين الـ Frame كاملا ثم يقوم بعمل Check for Errors عن طريق CRC
❖ Fragment Free	- يقوم بعمل Check علي أول 64 Bit فقط التي يحدث بهم الـ Error

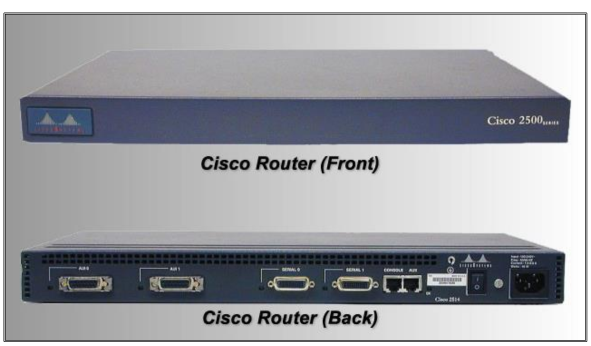


7- Router

- The Gateway for Devices
- يستخدم في ربط الفروع مع بعضها – Connecting More than Different Subnet
- Define the Best Way to Send Data Between Source and Destination
- لا يسمح بمرور رسائل الـ Broadcast ولكنه فقط يرسل رسائل الـ Unicast



هناك شركات تقوم بتصنيع Router يمكنك عمل اي Configuration تريدها عليها مثل CISCO and Juniper وهناك كورسات و Material حتي تستطيع ان تتعامل معها





من الأخطاء التي نقع فيها هو اننا بنقول علي الـ Device الموجود في المنزل مصطلح الـ Router لأنه ليس Router وإنما يسمي ADSL (Asymmetric Digital Subscriber Line)



8- ADSL

هذا هو شكل الـ Device المتواجد عندنا في المنازل
وظيفته انه بيعمل Modulation and De-Modulation يعني بيحول الاشارة اللي جياله من الـسنترال الـ Analog – الي - الـ Digital علشان تقدر تتوصل مع أجهزة الكومبيوتر

بكل بساطة:-

- اغلبيه الأنواع لا تقوم بعمل Connecting More than Different Subnet وهذه هي أهم مميزات الـ Router (هناك انواع Support Routing Protocols)
- وأيضا اغلبيه الـ Routers لا تملك من ضمن الـ Interfaces المتصله بها Input RJ-11 لتوصيل الخط الأرضي المسئول عن خدمة الإنترنت

هنا كتبت أغلبيه – حتي لا أعممها علي كل الأجهزة لأن هناك أجهزة يوجد فيها Input RJ-11 علشان يقوم بعملية التحويل من Digital to Analog Signal

DSL Type	Description
HDSL	(High-Bit-Rate DSL) Standardized in 1994, HDSL uses two pairs of 24 AWG copper wires to provide symmetric E1/T1 data rates to distances up to 3657 meters. Its successors are HDSL2 and HDSL4, the latter using four pairs of wire instead of two
SDSL	(Symmetric DSL) SDSL succeeded HDSL as the two-wire (single-pair) type of symmetric DSL. SDSL is also known within ANSI as HDSL2. Essentially offering the same capabilities as HDSL, SDSL offers T1 rates (1.544 Mbps) at ranges up to 10,000 feet designed for business applications.
ADSL	Asymmetric DSL ADSL provides transmission speeds ranging from downstream/upstream rates of 9 Mbps/640 kbps over a relatively short distance to 1.544 Mbps/16 kbps as far as 18,000 feet.

SHDSL	Single-Pair, High-Speed Digital Subscriber Line Also known as G. SHDSL, this type of DSL transmits data at much higher speeds than older types of DSL. It enables faster transmission and connections to the internet over regular copper telephone lines than traditional voice modems can provide. Support of symmetrical data rates makes SHDSL a popular choice for businesses using PBXs, private networks, web hosting and other services. SHDSL can be used effectively in enterprise LAN applications. Ratified as a standard in 2001, SHDSL combines ADSL and SDSL features for communications over two or four (multiplexed) copper wires. For higher-bandwidth symmetric links, newer G. SHDSL devices for four-wire applications support 10-Mbps rates at distances up to 1.3 miles (2 km). Equipment for two-wire deployments can transmit up to 5.7 Mbps at the same distance. SHDSL (G. SHDSL) is the first DSL standard to be developed from the ground up and to be approved by the International Telecommunication Union (ITU) as a standard for symmetrical digital subscriber lines. It incorporates features of other DSL technologies, such as ADSL and SDS, and is specified in the ITU recommendation G.991.2.
VDSL	Very-High-Bit-Rate DSL Also approved in 2001, VDSL as a DSL service enables downstream/upstream rates up to 52 Mbps/16 Mbps. Extenders for local networks boast 100-Mbps/60-Mbps speeds when communicating at distances up to 500 feet (152.4 m) over a single voice-grade twisted pair. As a broadband solution, VDSL enables the simultaneous transmission of voice, data, and video, including HDTV, video on demand and high-quality video conferencing.
VDSL2	Standardized in 2006, VDSL2 provides higher bandwidth (up to 100 Mbps) and higher symmetrical speeds than VDSL, enabling its use for Triple Play services (data, video, voice) at longer distances. While VDSL2 supports upstream/downstream rates similar to VDSL, at longer distances, the speeds don't deteriorate as much as those transmitted with ordinary VDSL equipment.

طريقه توصيل الـ Internet الي المنزل ؟

هناك مصطلحان أساسيان لمعرفة كيف يتم التوصيل الي المنازل: -

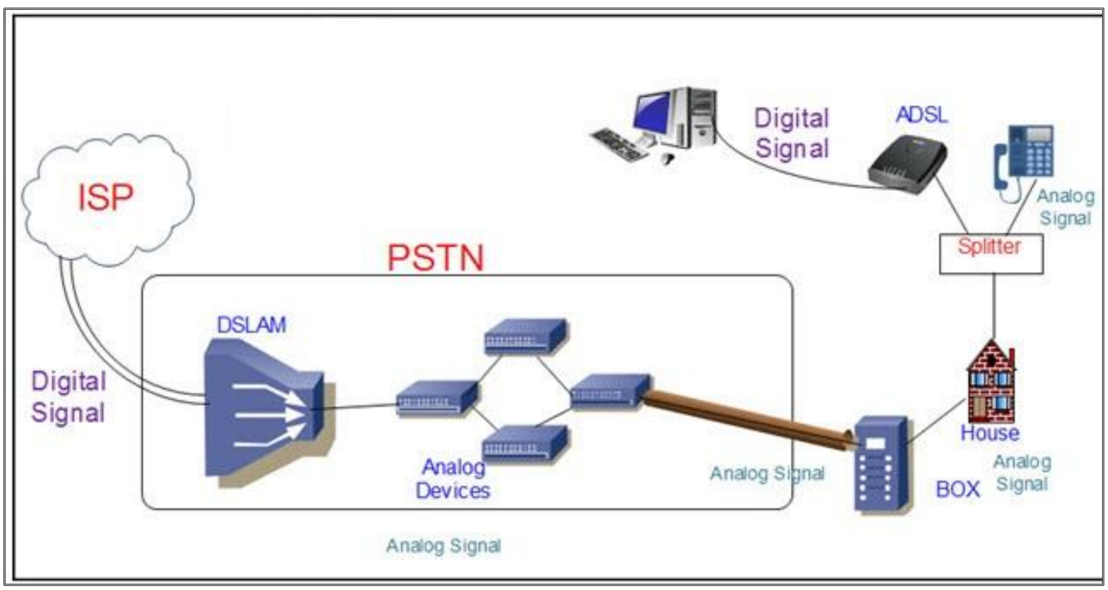
ISP → Internet Service Provider

وهي أي شركة من شركات مزودي خدمة الانترنت مثل :-

WE, Orange, Vodafone, etc,

PSTN → Public Switched Telephone Network

وهي اي شركه مسئولة عن خدمه التليفونات الأرضية كـ المصرية للاتصالات



لا توجد اي شركة ISP يمكنها توصيل Internet لأي عميل دون إذن من شركة الـ PSTN

يتم توصيل شركات الـ ISP بالـ DSLAM داخل السنترال او الـ PSTN عن طريق Fiber Cables

بعد ان يعاقد العميل مع الـ ISP تقوم هي بدورها بالاتصال مع المصرية للاتصالات وتحديد ما هو وضع البيت وهل هناك اي مشاكل في الخط حتي يسمح له بالتوصيل ام لا

هناك بعض المناطق النائية لا يسمح فيها بالسرعات العالية للإنترنت – لأن الـ Analog Cables مش بتقدر تستحمل الضغط العالي والسرعات الزيادة

9- DSLAM

DSLAM → Digital Subscriber Line Access Multiplexer

من اهم الأجهزة الموجودة في اي سنترال او اي شركة تعمل كـ PSTN



- يقوم بتحويل الـ Digital Signal الي Analog Signal حتي يتم توصيلها من خلال السنترال لأنه يتعامل مع الـ Analog فقط
وهو المسئول عن توصيل خطوط الربط وخطوط الانترنت للشركات المختلفة

يتم ارسال الـ Analog Signal من خلال كابلات الـ PSTN حتى تصل الي الـ Box المتواجد أسفل كل بيت Customer Premisesمرورا بالحائط حتى يخرج ويتم توصيله بما يسمي Splitter

من أهم عيوبه انه يقوم بعمل Share للـ Bandwidth
حيث انه اذا كان هناك 4 او 5 خطوط متصلين به – وهناك خط الـ Load عليه أقل من الآخر – يتم اخذ منه سرعة وتوزيعها علي الخطوط الـ Over Loaded حتي يستطيع ان يتعامل مع الضغط الغير محتمل



10- Splitter

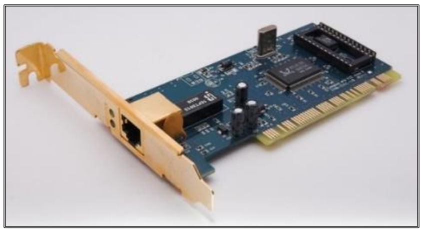
- يقوم بفصل الإشارة الي اثنين
احداهما الي التليفون الأرضي والأخرى الي الـ ADSL

وحتي هذه اللحظة كل هذا عبارة عن Analog Signal ولكن ; الـ PC يتعامل مع الـ Digital Signal

- لذلك يقوم الـ ADSL بعمل العملية العكسية وهي تحويل الـ Analog الي Digital
- وأيضا يقوم بعمل منع للتشويش الذي يحدث عند إجراء اي مكالمات أرضية

Digital Signal → Using RJ-45 | Analog Signal → Using RJ-11

الـ Router لا يقوم بأي من هذه الوظائف



11- NIC (Network Interface Card)

Ethernet
Physical Address
MAC Address

الذي يتم توصيله بالـ Switch او الـ ADSL Modem حتي استطيع ان اتصفح الـ Internet



12- Personal Computer

من أهم المكونات الأساسية لعمل أي شبكة سواء كانت LAN او WAN
يعتبر هو العنصر الأساسي والمهم في عمل اي نوع من انواع الـ Network

13- Server



- جهاز له امكانيات خاصة من حيث الـ Hardware
- حيث يستخدم لعمل Active Directory - Internal Domain حتي يتم التحكم في كل الأجهزة الخاصة بالشركة – ويمكن من خلاله ايضا عمل File Server حتي يتم تخزين كل الـ Important Data لتجنب فقدانها
- اي موقع يتم التعامل معه او الدخول عليه هو في الاساس Published من خلال Server عليه كل البيانات والداتا والمعلومات الخاصة بكل المستخدمين

مثلا كالـ فيس بوك – هناك آلاف السيرفرات التي تخدم على هذا الموقع

- السيرفرات ليها اكتر من نوع منها الـ Tower والـ Land Scape كـ Hardware وبيتم تنزيل عليها OS علي حسب استخدامك او متطلبات الشركة زي ESXI , Microsoft , Linux



Access Point

تستخدم لتقوية اشارة الـ Wireless - Wifi
وايضا تحويل الـ Wired Device الي Wireless
يمكن ايضا ان تجد لها مسميات أخري
WNAP → Wireless Network Access Point
NAP → Network Access Point

حاليا بقي في حاجه اسمها wireless LAN Controller عشان يتحكم في كل الـ Access Points



14- IP Phone

- Phones that Connected Using RJ-45 not RJ-11
- Phones يتم استخدامها لإجراء اي مكالمة سواء كانت محلية او دولية من خلال الـ ISP وليست الـ PSTN
- وتعتبر تكنولوجي VOIP حل مثالي جدا للشركات الكبيرة التي تمتلك اكتر من فرع في اكتر من محافظه او اكتر من دولة

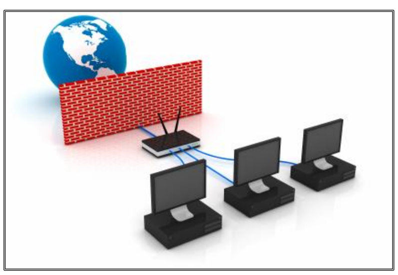
هل تمتلك Accountعلي Skype او هل انت من مستخدمي Telegram؟
هل حدث في مرة من المرات حينما قمت بدفع اشتراكك قام المسئول بإخبارك ان هناك تكلفة اضافية لمكالمات viper او Skype!! بالطبع لا
لأنه تم حسابها من ضمن الاشتراك المخصص لـ Internet Service -وهكذا مع الـ IP Phone Communication



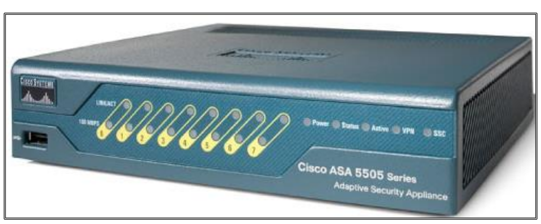
15- Multi-layer Switch

وهو Switch يمكنه ان يقوم بنفس وظائف الـ Router
وجاء مسمي Multi-Layer لأنه يمكنه ان يعمل في Layer 2 الخاصة بالـ Switch وأيضا Layer 3 الخاصة بالـ Router
اللي هيا الـ Routing Protocols and Services

16- Firewall



- يستخدم للتحكم في استخدام الموظفين للـ Internet
- عن طريق إجراء وتطبيق بعض الـ Restricted Roles علي كل الـ Users حتي نقوم بعمل Centralize للـ Service
- يمكن من خلاله منع بعض الـ Protocols من ان يتم استخدامها – Application من ان يتم التعامل معها – بعض الـ Service and Ports من ان يتم الاتصال بها
- To Prevent Any Outside External Threats



وأيضا في عمل اعدادات VPN Site to Site and Remote Access

Cisco ASA Firewall

أيضا هناك بعض الشركات الأخرى كـ Juniper , Forti and Palo Alto

17- IPS and IDS

Intrusion Prevention System – Intrusion Detection System



- من أهم أجهزة الحماية في اي Network
- عبارة عن أجهزة تعمل كـ Sensors حساسات في الشبكة
- أي اتصال غير مسموح به – أي Error – اي Packet حجمها اكبر من الطبيعي | بتم التعامل معها عن طريق Internal Database موجوده بداخلهم علي حسب الـ Category

- الفرق بين الـ نوعين :-

هو ان الـ IDS يقوم بعمل Alert فقط او عمل Detect للـ Error

اما الـ IPS يقوم بعمل Action و هو عمل Drop للـ Packet او اي شئ آخر علي حسب الـ Configuration التي تم اعداده من أجلها

- Error المقصود بها هنا :- Any Malicious - Up normal Connection

أغلبية أنواع الـ Firewalls حاليا بيكون فيها Bulit-in IPS وبيتقال عليها NGFW

This Page Intentionally* Left *Blank

Network Models

حضرتك الجهاز بتاعك بيكون شغال بـ OS معين ايا كان نوعه ايه ! من خلاله ممكن تفتح Facebook او انك تعمل شات بينك وبين اي حد بيستخدم موبايل !

طب مسألتش نفسك ازاي الأجهزة المختلفة دي ممكن تتكلم مع بعض ؟؟ ايه هيا الفكرة اننا مش بيطلع عندنا Error ان الحاجات الكتير المختلفة دي Not Compatible مع بعضها ؟

من هنا جت فكرة الـ Network Models – انها تسمح للـ Service المختلفة انها تتكلم مع بعض – عن طريق بعض الـ Standard Roles بتكون ثابتة علي كل الأجهزة أيا كان نوعها ايه

زي الـ Tour Guide اللي بيكون مع الفوج السياحي – لو مش فاهم كذا لغة مش هيعرف يتكلم مع كل الناس اللي موجودين

Models → To Allaw Different OS – Devices – Services – Infrastructure to be Communicated

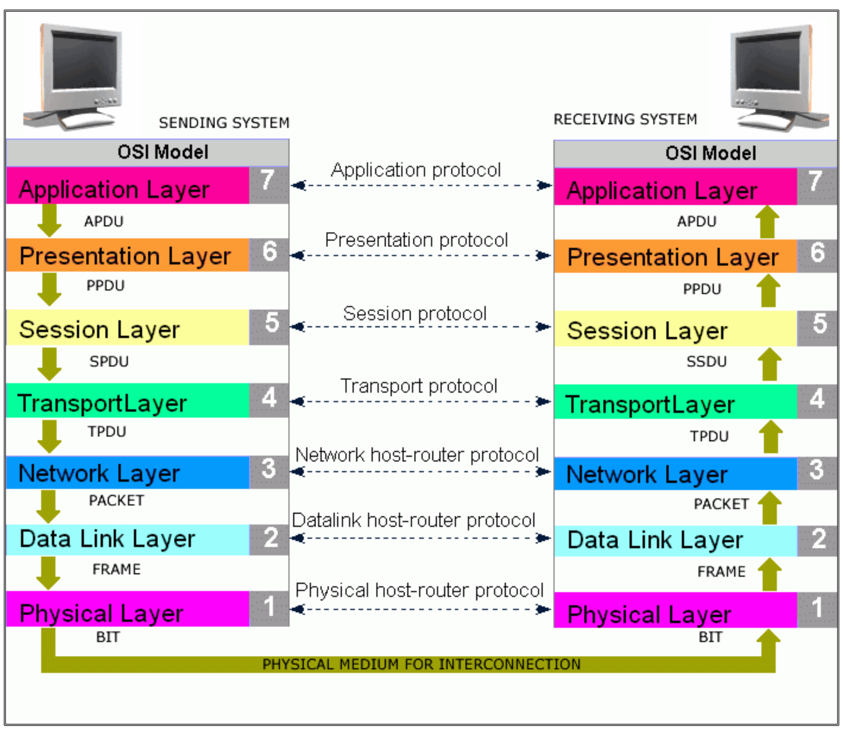
انواع الـ Network Models :-

OSI Model TCP/IP Model

- نبدأ نتكلم علي " OSI Model "Open System Interconnection – Intermediate :-

المنظمة اللي ابتكرته الـ "ISO "International Organization for Standardization

عباره عن 7 Layers هما المسؤولين عن نقل الداتا من الـ source للـ Destination



كل Layer مسؤولة عن عملية معينة في نقل الـ date او نقدر نقول انها بتقدم خدمة معينة بتستخدم في نقل الداتا وتسهيل عملية الـ communication اللي هتتم بين الأجهزة

Sending = Source Receiving = Destination

1- Application Layer :-

دي الـ Layer المسئولة عن تقديم اي خدمة الـ User بيحتاجها سواء كان انه يبعت Email لجهاز تاني او انه يعمل Download لأغنية عايز يسمعها او انه يعمل Browsing لأي موقع زي الفيس مثلا

طب ايه هيا الخدمات دي ؟؟

كل خدمة من الخدمات اللي بتقدمها الـ Application Layer بيكون ليها Port Number وليها Protocol مسئول عنها

الـ Port Number دا عبارة عن رقم ثابت للخدمة اللي انت بتعمل عليها Request – وبستخدمه علشان اعرف الـ Users اللي عندي في الـ Network إيه الخدمات اللي بيعملو ليها Access

ولو عايز امنع اي User من إنه يعمل Access لأي Service – بقفل الـ Port Number بتاعه من الFirewall وبتالي بيحصل للـ service دي Disable

او عن طريق الـ Access List – في كورس CCNA

Protocol	Stand foe :-	Port	Feature
HTTP	Hypertext Transfer Protocol	80	المسئول عن خدمة الـ Browsing لأي موقع حضرتك بتعمل عليه Connect علشان تشوف What is New ؟ ايا كان الموقع اللي حضرتك بتفتحه لازم يكون البروتوكول دا شغال حتي هتلاقي الموقع عندك بيكون دا شكل الـ URL بتاعه http://www.xyz.com
HTTPS	Hypertext Transfer Protocol Secure	443	نفس الـ HTTP بس الفرق في الـ Security اللي بيقدمها البروتوكول دا – في ان الداتا اللي بتتبعت بيحصل ليها عمليه تشفير " TLS or SSL" SSL → Certificate Type TLS → Encryption Type
DNS	Domain Name System or Server or Service	53	من أهم البروتوكولات كل موقع حضرتك بتـ Connect انت بتعمل اتصال بإسم الموقع – بس الجهاز بتاع حضرتك ميعرفش ايه هو الإسم دا هو يعرف حاجة اسمها الـ IP اللي هو العنوان بتاعه علي الشبكة . بالإضافه لكدا ان اي موقع او اي جهاز بيكون ليه حاجة اسمها IP - حضرتك لما بتيجي تتصل بأي شخص موجود عندك في الـ Phone Contact انت بتعمل Search علي الإسم بتاعه وبعد كدا بتعمل Dial نفس الفكرة مع المواقع – علشان نعمل Connect علي اي موقع لازم تكون حافظ الـ IP بتاعه – بس دا صعب جدا انه يتحقق

			- فالـ DNS بيقوم بالوظيفة دي بدل من حضرتك انه بيحول ليك من اسم الموقع اللي بتعمل Connect عليه --> للIP بتاعه علشان تتم عملية الاتصال بتاعك بكل سهولة والعكس Resolving from Name to IP
DHCP	Dynamic Host Configuration Protocol	67 – 68 (IP v4) 546 -547 (IP v6)	مسئول انه يقوم بعملية Assign لـ TCP/IP Configuration بطريقه Automatic يعني بدل ما تروح علي كل جهاز في الشركة اللي حضرتك فيها وتعطي الأجهزة الـ Network Configuration بطريقة Static – لا الـ Protocol دا بيوفرلك طريقه Automatic
SMTP	Simple Mail Transfer Protocol	25	مسؤول عن خدمة Email Sending يعني حضرتك لما بتبعت اي Mail لأي حد تاني بتستخدم البروتوكول دا عشان تبعت بيه
POP2	Post Office Protocol Version 2	109	مسؤول عن Receiving Mails المبعوتة من الـ Source للـ Destination
POP3	Post Office Protocol Version 3	110	مسؤول عن Receiving Mails المبعوتة من الـ Source POP2 Update
SNMP	Simple Network Management Protocol	161-162	مسؤول عن عمليات الـ Analysis – Monitor اللي بتستخدمها برامج الـ Network علشان تقيس مدي الكفاءة بتاعه الشبكة بتاعتك ومسؤول انه يكتشف اي خطأ ممكن يحصل وازاي تعالجه من اشهر الشركات اللي بتقدم Apps في المجال بتاع الـ Monitoring شركة اسمها Solarwind
FTP	File Transfer Protocol	20	بيقدم خدمة الـUploading & Downloading للملفات ايا كان الموقع اللي حضرتك بترفع عليه ملفاتك بتكون شغالة بالبروتوكول دا PN 20 مسؤول عن انه Open Session بين الـ Source and Destination
FTP	File Transfer Protocol	21	PN 21 مسؤول انه يعمل Start Uploading Process and Apply Security علي الملفات اللي بتترفع
TFTP	Trivial File Transfer Protocol	69	نفس الفكره بتاعه FTP بس كان فيه عيوب :- انه بيستخدم مع الملفات اللي حجمها صغير بس وان مكنش فيه Security and Browsing علشان كدا طوروه وعملوا FTP
Telnet	Remote terminal Access Protocol (unencrypted text communications)	23	بيقدم لينا خدمة Remote Connection علي الأجهزه سواء كانت Router – Switch - …etc. المشكله الموجودة في البروتوكول دا ان الـ Username and Password بيتبعتو As Clear Text فبإستخدام اي Hacking Tool like Wireshark ممكن اعمل تعقب لل Connection واعرف ال User and Pass

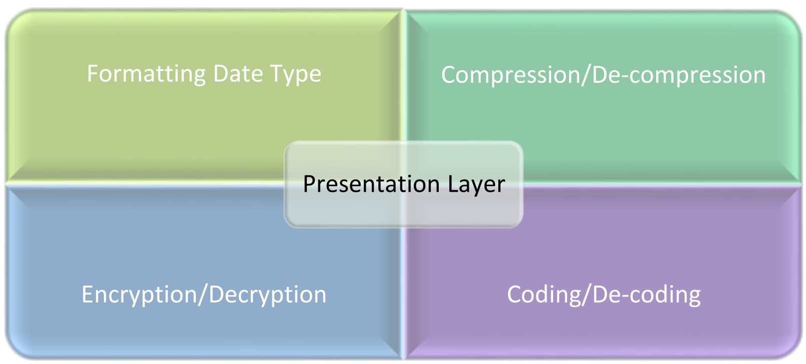
SSH	Secure Shell (SSH)	22	نفس الـ Telnet بس عالج المشكل اللي كانت فيه انه بيقوم بعمل تشفير للداتا المرسلة وكمان بيشفر الـ Username and Password
RTP	Real Time Transport Protocol	16384 - 32767	بيستخدم مع ال VOIP Tech

كل دي Service حضرتك بتستخدمها يوميا وانت مش واخد بالك هو ايه اللي بيحصل او حتي ازاي بيحصل دا كله وتقدر من الـ CMD بتكتب امر netstat او netstat -n علشان تقدر تشوف الـ Open Ports اللي عندك

دي أهم الـ Protocols اللي المفترض ان حضرتك تكون عارفها – مش كل الـ Protocols تم تناولها

Q : ايه الفرق بين IMAP and POP3 ؟؟

2- Presentation Layer :-



1- Coding/De-coding

هي عملية تحويل اي داتا بتتبعت بين الأجهزة الي 1 & 0 ودي اللغة اللي بتفهمها الـ Machine بتاعتك "Binary" علشان الداتا تقدر توصل بين الأجهزة ايا كان نوعها

Coding → on Source Machine   De-Coding → on Destination Machine

بعد ما بتتحول لـ Binary لازم الـ Destination يرجع ال Binary دا لكلام علشان ال User يقدر يفهم ايه المبعوت ليه

2- Encryption / Decryption

عمليه تشفير الداتا اللي بتتبعت بين الأجهزة – كنوع من انواع الـ Security اللي ممكن تضاف علي الداتا

الـ Presentation Layer بتستخدم MD5 في عمليه التشفير "Message Digit ver.5"

الـ Source بيقوم بعمليه التشفير -- وعملية فك التشفير الحاصل علي الداتا بيكون من مسؤولية Destination

3- Compression/De-compression

بيحصل ضغط للداتا المرسلة بين الأجهزة علشان نقلل حجمها وكمان نقلل استهلاك الـ Bandwidth المستخدمة

Bandwidth → سرعة نقل الداتا جوة الشبكة – علي حسب الجهاز المتوصل

4- Formatting Data Type

اني ممكن اتحكم في طبيعة الداتا اللي ببعتها او بستقبلها Extensions زي اللي بيحصل لما بنيجي نحمل فيديوهات من الـ YouTube

3- Session Layer

لو انت فاتح من الـ Browser بتاعك كذا Tab مثلا facebook – twitter – soundcloud
وجيت تعمل Refresh علي ال Tab بتاعه ال Facebook ايه اللي هيظهرك في ال Tab دي ؟؟
طبيعي هتقول ال Time line for Facebook !! طب ازاي ؟!!

هي دي بقي وظيفة الـ Session Layer انها تبعت الداتا علي حسب هيا مبعوتة من انهي Service علشان كدا مبيحصلش اي نوع من انواع الـ Errors
دي اول وظيفة من وظائف الـ Session layer اللي هيا Control Sessions
تاني حاجة من وظائفها – انها بتعمل Open Connection بين الـ Source والـ Destination
بعد الانتهاء عملية الاتصال بتعمل Close for Connection

الـ Session Layer هي اول Layer بيحتك بيها الـ Users علشان من غير ما نعمل Open Connection مفيش اي Service هتتم من الاساس .

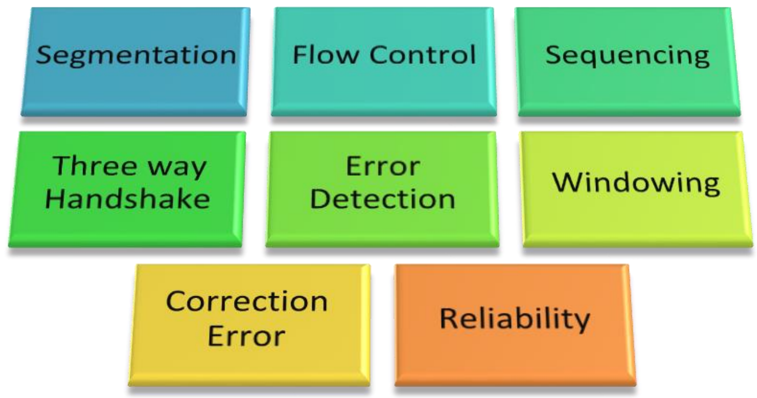
4- Transport Layer

من اهم الـ Layers بل تعتبر هي الـ Backbone Layer
اول Three Layers الـ Data بتكون فيها *as Data* يعني محصلش عليها اي Encapsulation يعني محصلش عليها اي إضافات تانية *"Headers"*
الـ Transport Layer هي اول Layer في عملية الـ Encapsulation
لما اتكلمنا في الـ Application Layer قولنا ان دي الـ Service اللي بنستخدمها – بس كل Service ليها نوع معين في الاستخدام هل بتعتمد علي الـ Security وان الداتا توصل كاملة ولا بتعتمد علي السرعة فقط

بييجي هنا مصطلحين مهميين اوي TCP UDP
وهما دول اللي بيحددو نوع الـ Service اللي بنستخدمها
اول ما بنضيف نوع الـ Service علي الـ Data بتتحول لـ Segment

TCP “Transmission Control Protocol “	"UDP "User Datagram Protocol
بتكون فيها الداتا بتعتمد علي الـ Security والـ Reliability يعني انها توصل كاملة ولو حصل اي Error في عملية نقل الداتا يتعمل ليه Detect and Correct وبتعمل كمان حاجة اسمها Flow Control يعني ان معدل النقل يكون مناسب لكل الأجهزة اللي بتتكلم مع بعض زي اي عملية Connection بنستخدمها كـ Users سواء Uploading – Email Service	بتعتمد علي السرعة فقط بتستخدم حاجة اسمها Real Time يعني اللي بيحصل عند الـ Destination الـ Source بشوفه لحظيا زي اي Live Matches or Live Broadcasting واي مكالمات بتم باستخدام الانترنت علي أي Application لو بتتفرج علي ماتش اونلاين وحصل اي Error في الانترنت – هل لما النت بيتظبط الماتش بيستني عند الحتة اللي حصل فيها ال Error ولا بيكمل عادي وبيسيب اللي فات ؟ ودي بتستخدم اكتر مع الـ Voice and Video Over IP

وظائف الـ Transport Layer :-



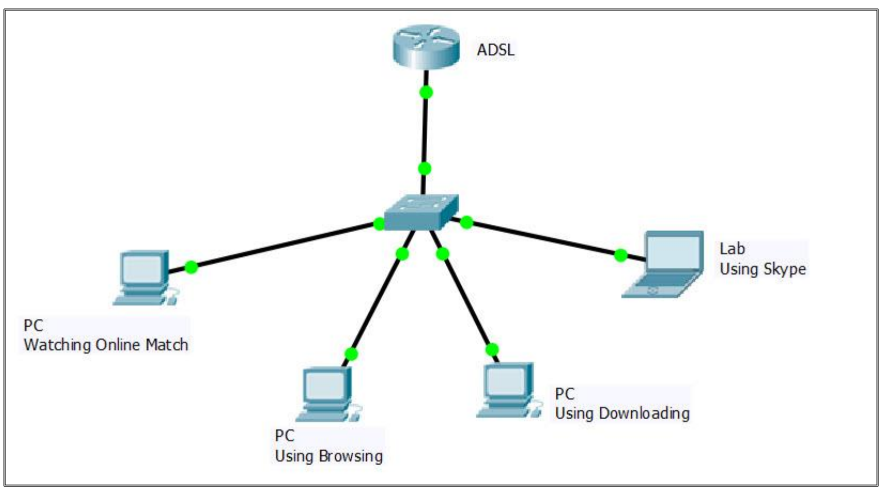
1- Segmentation

قولنا ان اسم الـ Data في الـ Transport Layer بتكون Segment بيكون حجمها كبير بالنسبة لعملية Communication فعملية الـ Segmentation وظيفتها انها تقسم الـ Segment الكبيرة لمجموعة Segments صغيرة . طب ليه ؟

اولا : علشان تتبعت بسرعة

ثانيا : علشان لو حصل Error في جزء معين اعرف اعمل ليها Detect and Correct بسهولة بدل ما اعمل للـ Segment الكبيرة كلها

ثالثا : علشان لو عندي اكتر من Service



لو عندي اكتر من Service زي اللي موجودة بالشكل دا – هنلاقي في حاجات بتعتمد علي TCP و بعضهم بيعتمدوا علي الـ UDP

لو مثلا الجهاز اللي بيعمل Download دا هو اول جهاز بعت الـ Request هيسحب الـ Traffic كله – بالتالي اللي بيستخدم Skype او Online Service مش هيستخدم الـ Feature بتاعة الـ Real Time

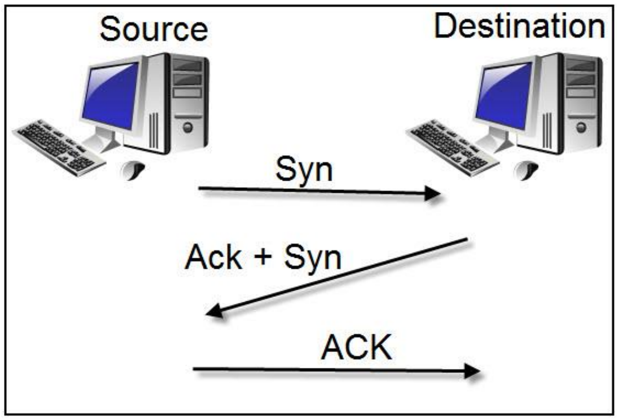
علشان كدا بيحصل عملية *Segmentation* علشان يحصل Mix بين الـ Segments ونحقق كل شروط نقل الـ Data

2- Sequencing

وهي عملية ترقيم للـ Segmentation اللي اتجزإت علشان الـ Destination يبقي عارف هو استلم قد ايه ولسه فاضل قد ايه ؟

Three Way Handshake -3

بتستخدم لغرض انها تعمل Test للـ Connection بين الـ Source والـ Destination عن طريق ارسال Synchronous and Acknowledge message بينهم

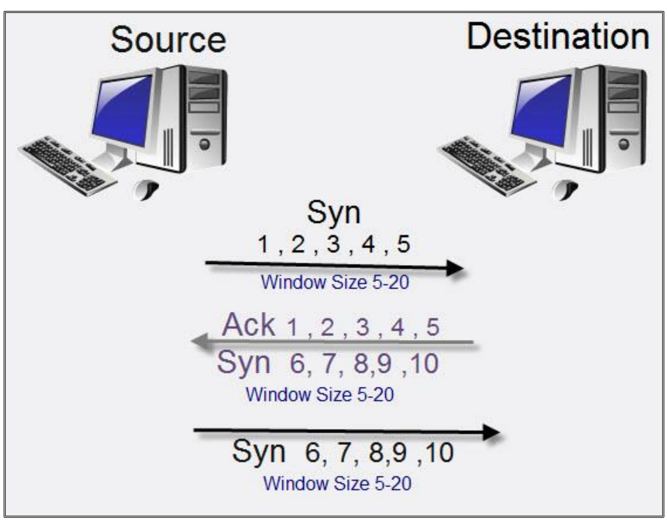


الـ Source بيبعت للـ Destination علشان يتفقوا علي عدد الـ Segments اللي هتتبعت ف كل مرة – الـ Source Msg بيكون اسمها Synchronous , ولو الـ Destination متاح واستلم الـ Segments دي بيرد علي الـ Source بـ Acknowledgement Msg وبيطلب منه باقي الـ Segment الباقية

لو عندي Segment حجمها 150 Byte وحصلها Segmentation وبقي كل Segment حجمها 10 Byte

يعني دا معناه ان هيكون عندي 15 جزء هيتبعتوا - - الـ Source بيحدد عدد عشوائي من الـ Segments علي حسب الـ Process بتاعته وبيبعتها للـ Destination وبيكون عندي كذا حالة في الموضوع دا :-

Case 1 :-



ان الـ Source هيحدد انه هيبعت 5 Segment في المرة ودي بيكون اسمها الـ Window Size
اللي هي عدد الـ Segments المبعوتة في المرة الواحدة من العدد الاجمالي

لو الـ Destination استلمهم كلهم هيبعت يقوله انه Ack وتمام وابعت

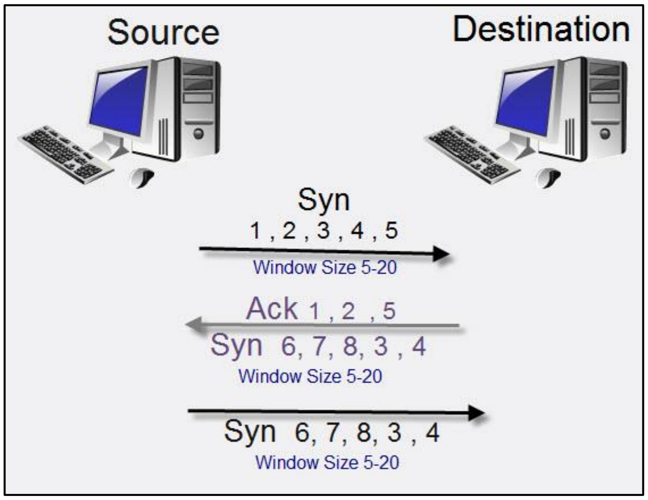
الـ 5 اللي بعدهم وهكذا

الـ Source بيعرف ان الـ Segments كلها وصلت من الـ Value بتاعه الـ Window Size

وبعد كدا تبدأ عملية الـ *Windowing* :-

اللي هي عملية بداية الإتصال الفعلي بينهم

-: Case 2



نفس طريقة الـ Source انه بيحدد عدد عشوائي وبيعت علي اساسه , ولكن هنا حصل عن لـ Error Destination في الـ Segments 3 , 4

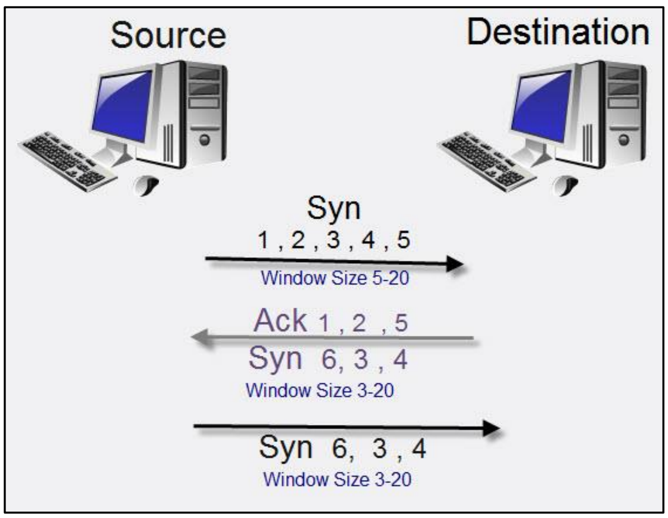
نتيجة لأي مشكلة في الـ Internet مثلا

بس حجم الـ Window Size فضل ثابت زي ما هو والـ Destination بعت للـ Source قاله ايه اللي استلمه وايه اللي لسه فاضل ليه

المسؤول عن اكتشاف وتصحيح الـ Errors هي الـ CRC

Cyclic Redundancy Check وظيفتها انها بتعمل Error Detect and Error Correct لو حصلوا علي الـ Segments المرسلة او المستلمة بين الأجهزة

-: Case 3



نفس طريقة الـ Source انه بيحدد عدد عشوائي وبيعت علي اساسه , ولكن هنا حصل عن لـ Error Destination في الـ Segments 3 , 4

ولكن الـ Error اللي حاصل هنا في مشكلة عند الـ Destination علشان حصل عنده Over Flow

معناه :- ان سرعة نقل الـ Date من الـ Source للـ Destination اكبر من معدل استيعاب الـ Destination للداتا المبعوتة

وبالتالي الـ Destination هيطلب من الـ Source انه يعدل الـ Window Size علي حسب مقدار استيعابه

الـ Destination هيعمل حاجة اسمها Flow Control انه هيتحكم في معدل ارسال الداتا اللي بتجيله من الـ Source

ودي الـ Case الوحيدة اللي بتتغير فيها الـ Window Size
وبرضه المسؤولة عنها هي الـ CRC

بعد كدا ايا كان الـ Case اللي حاصلة – كل دا بيتم في عملية Test for Connection

عملية بداية الـ Connection الفعلي اسمها Windowing

وبكدا نكون خلصنا كل وظائف الـ Transport Layer

5- Network Layer

تاني Layer بتضيف Encapsulation way علي الـ Data -- بتضيف الـ IP Address وبتحول الـ Segment لـ Packet
الـ IP هو عنوان الجهاز علي الشبكة او عنوان الموقع اللي انا عايز اعمل عليه Connect – هنتكلم عنه بالتفصيل في الشابتر الخاص بيه

وظائف الـ Network Layer :-

Routing Protocols

وظيفه الـ Routing Protocols انها تحدد افضل مسار في عمليه نقل الداتا بين الأجهزة

Define the Best Path - Route- Way to Send Data

وكمان وظيفتها انها تخلي الشبكات المختلفة تقدر تتكلم مع بعض
علشان الراوتر بيقدر يفهم اكتر من شبكة

Type of Routing Protocols :-

RIP
OSPF
EIGRP
BGP
هنتكلم عنهم بالتفصيل في Routing Track

Routed Protocols

مسؤولة عن عملية الـ Addressing يعني ازاي الجهاز بياخد IP بإختلاف الـ OS بتاعه

Types of it :-

IP --> Standard
IPX/SPX --> for Novell
Apple talk --> for Apple Decvices

Other Protocols

ARP

وظيفته انه بيجيب الـ IP Address بدلاله الـ MAC
والـ RARP بيقوم بالوظيفة العكسية ,

ICMP

وظيفته انه يعمل Testللـ Connection ويشوف الـ Destination متاح لا لأ

وممكن كمان نستخدمه علشان نشوف الانترنت شغال ولا لأ عن طريق اننا بنعمل

ping sitename وعلي حسب الـ Responce بنشوف ايه الوضع

1- Request time out

2- Destination host unreatchable

3- Reply from

Data Link Layer -6

بتحول الـ Packet لـ Frame عن طريق انها بتضيف الـ MAC Address بتاع الاجهزة

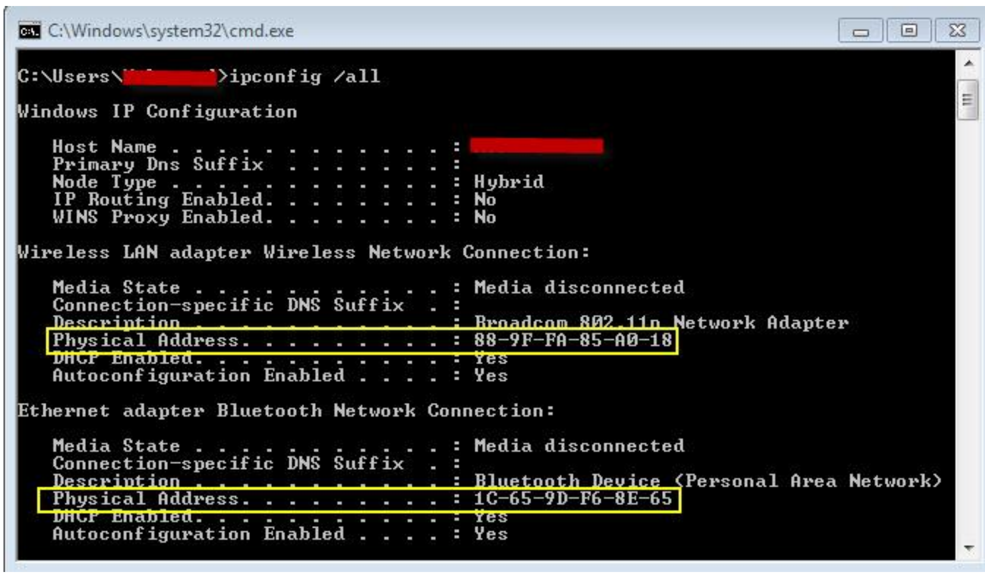
ايه هو الـ MAC ؟

الـ Physical Address اللي بيكون محفور علي الـ NIC بتاع الجهاز بتاع حضرتك , مينفعش الـ MAC بتكرر علي الأجهزة وبتالي هو Unique , بيتكون من 48 bit يعني 6 Byte اللي اخترعه هيا :-

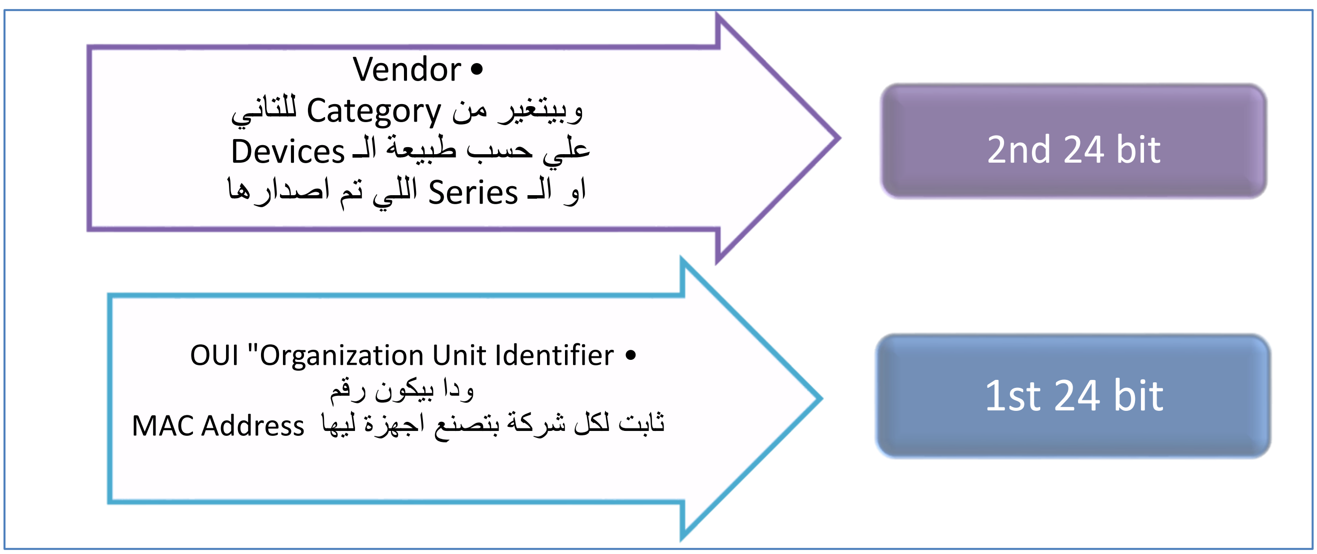
IEEE The Institute of Electrical and Electronics Engineers

مكتوب بلغة اسمها Hexa Decimal يعني بيتكتب بالارقام والحروف

علشان تعرف الـ MAC بتاع جهازك – علي الـ *CMD* هتكتب امر اسمه *ipconfig /all*



الـ MAC Address بيتقسم لجزئين



وتقدر تستخدم موقع زي MAC Address lookup علشان تتأكد من الـ OUI المصنعة للـ MAC Address بتاع جهازك

وظائف الـ Data Link Layer :-

1- Arbitration :-

انها كانت بتحدد ايه هو افضل وقت في عملية ارسال الداتا . وكانت اهميتها في الـ Bus and Ring Topologies

Define the Best Time for Sending Data

2- Error Detection

- Parity Check :-

بتحسب عدد الـ Bits اللي بتساوي 1 في الداتا المرسلة

ليها Two Algorithms شغالة بيهم :-

Even or Odd

لو انا بستخدم الـ Odd لازم عدد الـ Bits بتاعه الـ 1 يكون عدد فردي

لو هستخدم الـ Even لازم عدد الـ Bits بتاعه الـ 1 يكون عدد زوجي

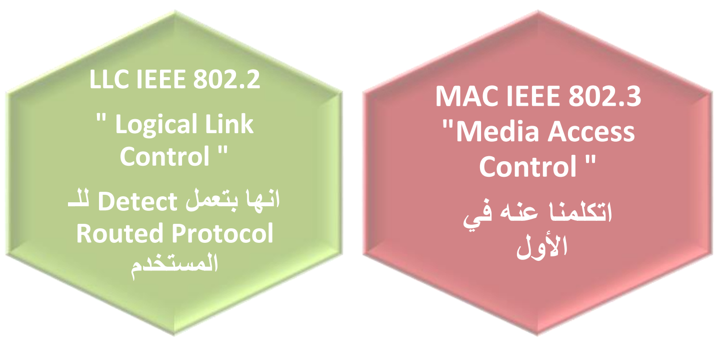
ممكن يحصل Error في عدد الـ Bits بتاعه الـ 1 وبتالي هيكون في ناتج تبع نفس الـ algorithm بس مش هنعرف نعمل ليه Detect بسهولة -- ومعدتش بتستخدم

CRC with FCS :-

الـ CRC في الـ Data Link Layer بتعمل Error Detect Only ومش بتعمل ليها اي Correct يعني لو حصل Error الـ User هيستلمه عادي علشان حصل بعد الـ Transport Layer

الـ FCS بتشتغل مع الـ CRC ليها نفس الطريقة بس الإختلاف انها بتضاف في الـ Tailer بتاع الـ Header

Data Link Sub Layers



7- Physical Layer

بتقوم بعمليه Coding للـ Header ككل وبتحوله لـ 0/1 علشان يتبعت في الـ Medium وبتبعت للـ Destination

وبيشتغل فيها اي أجهزة Not Smart وايضا الـ Cables

وبكدا عملية الـ Coding and De-Coding بتحصل مرتين في عملية نقل الـ Data

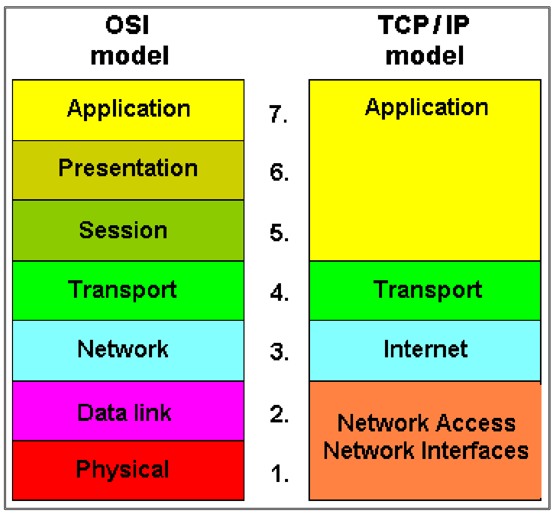
This Page Intentionally* Left *Blank

TCP/IP Model

المنظمة اللي ابتكرت الـ Model دا هي الـ <u>DOD " Department of Defense "</u>

علشان يكون اسرع من الـ OSI في عملية نقل الداتا – وكمان يكون كـ Backup ليه علشان لو حصل فيه اي مشاكل يكون في Standard ثابت لنقل الداتا

وتم اعتماده كنظام ثابت لكل الأجهزة



عبارة عن 4 Layers ليهم ليهم نفس الوظائف بتاعه الـ OSI بس الفكره ان الـ Process علي الداتا بقي اسرع

حصل دمج في بعض الـ Layers وتغيير في بعض اسماء Layers اخري

Application, Presentation and Session → Application

Network → Internet

Data link and Physical → Network Access or Network Interfaces

Encapsulation Techniques in Models:-

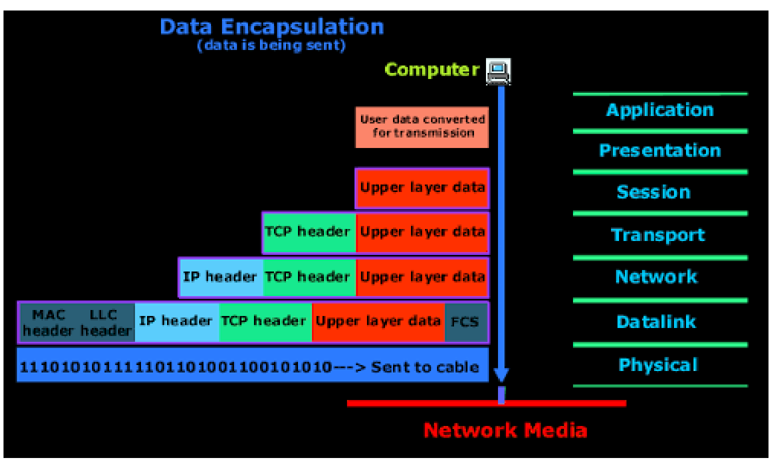
Encapsulation

OSI Layer	Wrapper Name	Header Name
Application	N/A	Layer 7 Header
Presentation	N/A	Layer 6 Header
Session	N/A Upper Layer Data	Layer 5 Header
Transport	Segment	TCP Header
		UDP Header
Network	Packet	IPv4 Header
		IPv6 Header
Data Link	Frame	Ethernet Type II Header
		IEEE 802.2 / 802.3 / 802.3 SNAP
		Other Frame Headers
Physical	Bits	N/A

- بتبدأ تحصل من اول الـ Transport Layer انها بتضيف نوع الـ Service اللي الـ User بيستخدمها وبتحول الـ Data لـ Segment
  بعد كدا بتيجي وظيفة الـ Network Layer انها بتضيف الـ IP Addresses والـ Routing and Routed Protocols علشان الداتا تتبعت في المسار الصحيح بتاعها وميحصلش ليها اي Failures , وبيتحول الـ Segment لــ Packet
- الـ Data Link Layer بتضيف الـ MAC Address في الـ Header وكمان بتضيف الـ FCS في الـ Tailer علشان الداتا يحصل ليها تغليف من الناحيتين وبتحول الـ Packet لــ Frame
- الـ Physical Layer بتعمل عملية Coding لكل الأجزاء دي اللي بتسمي الـ Header وبتحولها لـ 0/1 علشان تمشي في الـ Cables

- <u>عمليه الـ Coding بتحصل مرتين في عملية نقل الداتا :-</u>

مرة في الـ Presentation Layer وبتحصل علي الـ Data فقط – ومره تانية بتحصل في الـ Physical Layer وبتتم علي الـ Header ككل



Network Devices with its Layers

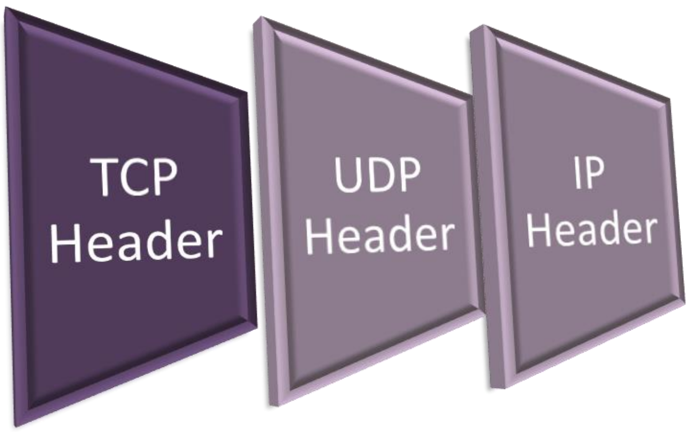
Device	Layer
Hub , Connector , Repeater , Cables	Physical Layer
Switch , Bridge , Access Point , NIC	Data Link Layer
Router , Multi-Layer Switch	Network Layer
IPS , IDS	Presentation Layer
Firewall	Filter All Traffics in All Layer
Server	It’s about the Service type that Provide

This Page Intentionally **Left** *Blank*

Headers

اتكلمنا في الـ Models علي ان بتحصل عملية Encapsulation علي الـ Data

ان بيحصل Add لـ Header بتاع الـ Service اللي بنستخدمها علشان تغلف الداتا وتحولها لإسمها في الـ Layer بتاعتها



TCP Header

- بيستخدم مع الـ Data اللي بتعتمد علي الـ Security and Reliability
- الحجم الإجمالي بتاعه 20 Byte
- بيتقسم لـ 32 bit العرض بتاعه – والطول 5 Byte

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Source Port          |       Destination Port        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Sequence Number                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Acknowledgment Number                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       |           |U|A|P|R|S|F|                               |
|  HL   | Reserved  |R|C|S|S|Y|I|            Window             |
|       |           |G|K|H|T|N|N|                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Checksum            |         Urgent Pointer        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Options                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             data                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

                       TCP Header Format
```

-: Source and Destination Port

الـ Port زي ما اتكلمنا عنه قبل كدا قولنا انه عبارة عن مدخل او مخرج الـ User للـ Service اللي هو عايز يعمل ليها Access لازم للـ User يكون ليه Port Number يخرج منه - عدد الـ Ports الإجمالي 65535

بتتقسم لـ :-

0 : 1023 ودا بيكون بتاع الـ Reserved Service , Public , Online اللي اتكلمنا علي جزء منهم في الـ Application Layer
1024 : 49151 ودول بيستخدموا في الـ New Technology واي إضافات في الـ Ports
65535 : 49152 ودول اليوزر بيستخدمهم في حالة الــ NAT وتحديدا في الـ PAT

-: Sequence Number

مسئول عن عملية الترقيم اللي بتتم علي الـ Segments اللي بيحصل ليها Segmentation علشان الـ Destination يبقي عارف استلم قد ايه وفاضل قد ايه -- حجمها 32 Bit

-:Acknowledgement

بتعمل Check علي ان الـ Segments كلها , هل وصلت للـ User كاملة ولا لأ ؟

-: Header Length

قيمة ثابتة وبيتحدد فيها ان حجم الـ Header ثابت انه 20 Byte

-: Reserved

جزء محجوز لأي Update ممكن يتضاف علي الـ Header في الـ Future Use

-: TCP Flags

بستخدمهم علشان اعمل Test للـ Connection بين الـ Source والـ Destination – بس ليهم كذا نوع وكل نوع ليه خدمة معينة بيقدمها

الـ Default Value بتاعة كل Flag منهم انها بتساوي 0 حتي يتم استخدامها

بالنسبة لـ URG – RST – PSH إستخدامها أكتر في عمليات الـ Hacking وفي شابتر كامل في كورس *C|EH* بيتكلم عنهم وازاي استخدمهم

في برامج بتخليني اقدر اتحكم في نوع الـ Flags اللي عايز استخدمه زي : NMAP

Flag Name	Service
Synchronous " SYN "	دا اللي الـ Source ببعته للـ Destination علشان يبدأ معاه عمليه الـ Connection
Acknowledgement " ACK "	الرد بتاع الـ Destination علي الـ SYN بتاعة الـ Source
Push " PSH "	بستخدمه في حالة لو انا عايز ابعت كل الـ Segments بتاعتي مرة واحدة بغض النظر عن الـ Window Size المتفق عليه بينهم علشان اعمل عند الـ Destination حاجه اسمها Over Flow

Urgent “ URG “	يستخدم في حالة ان عندي Segment محدده عايز ابعتها دلوقت ومش عايز اخليها تستني في الـ Queue بتاع الـ Segments
Reset “ RST ”	فايدته اني اعمل Reset للـ Connection إجباري عند الـ Destination
Finish “ FIN “	لو خلاص كل الـ Segments ابتعتت وتم استلامها ومعتش في اي غرض تاني من الـ Connection كل واحد منهم بيقفل الـ Connection وبتنتهي عمليه الاتصال

-: Window Size

دي اللي بتحدد فيها حجم الـ Header بالإضافة الي حجم الداتا المرسلة , الـ Data ملهاش حجم معين وهيا مش جزء من الـ 20 Byte بتوع الـ Header .

المسؤول عن عمل Detect لحجم الـ Data المرسلة هو الجزء بتاع الـ Window Size

-: Check Sum

ودي المسؤولة عن عملية الـ Error Detection and Correction اللي بتشتغل فيها الـ CRC

-:Urgent Pointer

لو حصل اي Error في أي جزء من أجزاء الـ Header , هي بتحل محله في الشغل , الحجم بتاعها 16 Bit .
وبالتالي لو حصل اي Error في جزء حجمه اكبر من حجم الـ urgent Pointer هتعتبر الـ Segment دي مرفوضة Rejected والـ Destination هيطلبها من الـ Source تاني

-: Option

دي بتخص اي OS – Infrastructure – Vendor علشان كل واحد منهم ليه Option مختلفة عن التاني فلازم يحصل ليها Add في الـ Header

-: Data

ودي الداتا المرسلة – ملهاش اي حجم ثابت في الـ Header بس زي ما وضحنا المسؤول عن اضافة حجمها في الـ Header هو الـ *Window Size*

UDP Header

- ❖ بيستخدم مع الـ Data اللي بتعتمد علي السرعة وشرط ارسالها هو الـ Real Time
- ❖ حجم الـ Header اجمالا 8 Byte , العرض 32 Bit والطول 2 Byte
- ❖ واللي واضح من الـ Diagram بتاعه ان في اجزاء كتير كانت في الـ TCP Header مش موجودة فيه علشان هو ملوش اي علاقه باي Security او حتي ان الداتا توصل كاملة او لأ .

0 — 15	16 — 31
Source Port Number(16 bits)	Destination Port Number(16 bits)
Length(UDP Header + Data)16 bits	UDP Checksum(16 bits)
Application Data (Message)	

-: Source and Destination Port

نفس الكلام اللي قولناه في الـ TCP Header

-: Length

هنا مختلفة عن الـ TCP , اللي بيساويها هناك هو الـ Window Size لأنها هنا بتحدد حجم الـ Header بالإضافة لحجم الـ Data المرسلة

-: UDP Checksum

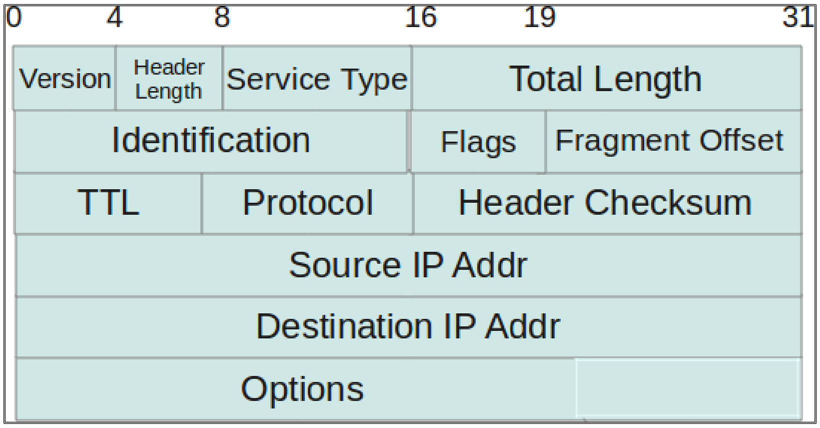
مسؤولة عن عمل Error Detect Only علشان تعرف الـ Destination ان حصل Error بس مبيحصلش ليه اي عملية Correction إطلاقا , وبرضه المسؤول عنها هي الـ CRC

-: Data

ودي الداتا المرسلة – ملهاش اي حجم ثابت في الـ Header بس زي ما وضحنا المسؤول عن اضافة حجمها في الـ Header هنا هو الـ *Header Length*

IP Header

دا اللي بيتضاف علي الـ Segment علشان يحولها لـ Packet -- الحجم بتاعه نفس حجم الـ TCP Header



-: Version

بتحدد هل الـ IP المستخدم دا IPv4 or IPv6

-: Header Length

بتعمل Detect لحجم الـ Header فقط اللي هو 20 Byte

-: " TOS " Type of Service

نوع الـ Service اللي هتتنقل باستخدام الـ IP وبتحدد الـ QoS Quality of Service وكمان بتحدد ازاي الـ Router هيتعامل مع الداتا اللي جياله , هل هيبعتها علي طول ولا هتستني في الـ Queue

ليها مصطلح تاني اسمه IP Differentiated Services Code Point (DSCP)

ToS Value	ToS Description
0 (000)	Routine
1 (001)	Priority
2 (010)	Immediate
3 (011)	Flash
4 (100)	Flash Override
5 (101)	CRITIC/ECP
6 (110)	Internet Control
7 (111)	Network Control

-: Total Length

ودي بتحدد حجم الـ Header بالاضافة لحجم الـ Segment المضافة ليه من الـ Transport Layer

-: Identification

قبل ما نتطرق ليها – في مصطلح اسمه *Maximum Transmission Unit* MTU ودا بيحدد ايه هو اقصي حجم للـ Packet ممكن تمر من الـ Device او الـ Interface – قيميتها انها بتكون *1500* Byte by Default

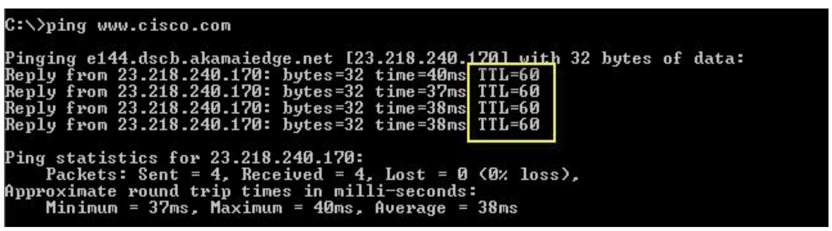
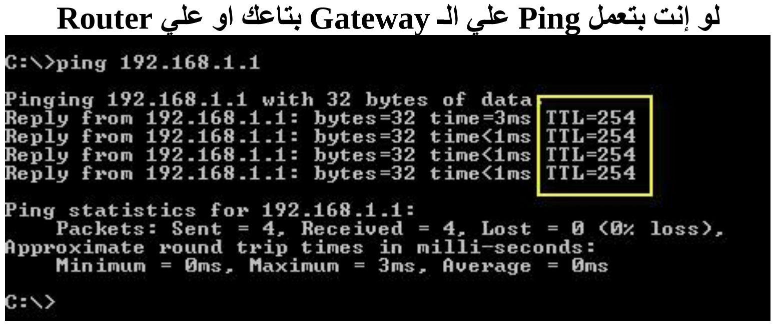
لو حصل والـ User بعت Packet حجمها اكبر من الـ MTU الـ Router المفروض انه هيعمل ليها Reject !! لأ طبعا !!

الـ Router هيعمل ليها حاجة اسمها *Fragmentation* يعني هيجزئها – وهيعطي لكل جزء ID علشان عملية الترقيم ليهم وهيجمع كل مجموعة Fragments مع بعضها بحاجة اسمها *Flag*

علشان تقدر تمر منه وتوصل للـ Destination -- وبكدا نكون اتكلمنا عن الـ **Fragment Offset – Identification – Flags**

-: TTL

Time to Live فترة حياة الـ Packet اللي هتفضل تلف فيه وتدور علي الـ Destination بتاعها او يحصل ليها Drop – الـ Packet مش هتفضل تلف كدا في الفاضي في الشبكة علشان ميحصلش Loop

TTL Default Value	**Why**
64	في حالة لو انت بتعمل Ping علي أي Online Site وفي الحالة دي الناتج اللي بيكون موجود الفرق بينه وبين 64 هو عدد الـ Hops اللي عدت عليهم  C:\>ping www.cisco.com Pinging e144.dscb.akamaiedge.net [23.218.240.170] with 32 bytes of data: Reply from 23.218.240.170: bytes=32 time=40ms TTL=60 Reply from 23.218.240.170: bytes=32 time=37ms TTL=60 Reply from 23.218.240.170: bytes=32 time=38ms TTL=60 Reply from 23.218.240.170: bytes=32 time=38ms TTL=60 Ping statistics for 23.218.240.170: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 37ms, Maximum = 40ms, Average = 38ms
128	**في حالة لو انت بتعمل Ping علي جهاز شغال معاك علي نفس الـ LAN بتاعتك واحيانا في الـ Public IP Testing**
256	**لو إنت بتعمل Ping علي الـ Gateway بتاعك او علي Router**  C:\>ping 192.168.1.1 Pinging 192.168.1.1 with 32 bytes of data: Reply from 192.168.1.1: bytes=32 time=3ms TTL=254 Reply from 192.168.1.1: bytes=32 time<1ms TTL=254 Reply from 192.168.1.1: bytes=32 time<1ms TTL=254 Reply from 192.168.1.1: bytes=32 time<1ms TTL=254 Ping statistics for 192.168.1.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 3ms, Average = 0ms C:\>

لو انا عايز اشوف ايه هيا الـ Hops اللي عدت عليهم الـ Packets اللي بعتها علشان توصل للـ Destination بستخدم بروتوكول من ضمن الـ Network Layer Protocols اسمه tracert بيعمل تعقب للـ Packets المبعوته اللي هيا Trace Route

الفرق بين قيمة الـ TTL والفيمة الـ Default بتاعتها – هي عدد الـ Hops اللي عدت عليها الـ Packet علشان توصل للـ Destination بتاعها

```
C:\>tracert www.cisco.com

Tracing route to e144.dscb.akamaiedge.net [23.218.240.170]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  192.168.1.1
  2    48 ms    51 ms    42 ms  172.31.1.200
  3    34 ms    31 ms    32 ms  172.21.29.181
  4    39 ms    38 ms    39 ms  172.21.16.222
  5    39 ms    38 ms    39 ms  a23-218-240-170.deploy.static.akamaitechnologies
.com [23.218.240.170]

Trace complete.
```

-: Protocols

نوع الـ Protocol المنقول بإستخدام الـ Header - في آخر الشابتر هيكون في توضيح لكل الـ Protocols المستخدمة وايه هيا الـ Values بتاعتها

-: Header Checksum

مسؤولة عن عمل Error Detect Only لو حصل في اي Packet

-: Source and Destination IP

عناوين الأجهزة اللي بتعمل Connect مع بعضها علشان الـ Packet تبقي عارفه هيا راحة من مين لفين

-: Options

لو في اي اضافة هتحصل علي الـ Header دا – نفس الكلام الذي تم ذكره في الـ TCP Header

IP Header "TOS" - for Read only

Value	Protocol	References
0	HOPOPT, IPv6 Hop-by-Hop Option.	RFC 2460
1	ICMP, Internet Control Message Protocol.	RFC 792
2	IGAP, IGMP for user Authentication Protocol. IGMP, Internet Group Management Protocol. RGMP, Router-port Group Management Protocol.	RFC 1112
3	GGP, Gateway to Gateway Protocol.	RFC 823
4	IP in IP encapsulation.	RFC 2003
5	ST, Internet Stream Protocol.	RFC 1190, RFC 1819
6	TCP, Transmission Control Protocol.	RFC 793
7	UCL, CBT.	
8	EGP, Exterior Gateway Protocol.	RFC 888
9	IGRP, Interior Gateway Routing Protocol.	
10	BBN RCC Monitoring.	
11	NVP, Network Voice Protocol.	RFC 741
12	PUP.	
13	ARGUS.	
14	EMCON, Emission Control Protocol.	
15	XNET, Cross Net Debugger.	IEN 158
16	Chaos.	
17	UDP, User Datagram Protocol.	RFC 768
18	TMux, Transport Multiplexing Protocol.	IEN 90
19	DCN Measurement Subsystems.	
20	HMP, Host Monitoring Protocol.	RFC 869
21	Packet Radio Measurement.	
22	XEROX NS IDP.	
23	Trunk-1.	
24	Trunk-2.	
25	Leaf-1.	
26	Leaf-2.	
27	RDP, Reliable Data Protocol.	RFC 908
28	IRTP, Internet Reliable Transaction Protocol.	RFC 938
29	ISO Transport Protocol Class 4.	RFC 905
30	NETBLT, Network Block Transfer.	
31	MFE Network Services Protocol.	
32	MERIT Internodal Protocol.	

33	DCCP, Datagram Congestion Control Protocol.	
34	Third Party Connect Protocol.	
35	IDPR, Inter-Domain Policy Routing Protocol.	
36	XTP, Xpress Transfer Protocol.	
37	Datagram Delivery Protocol.	
38	IDPR, Control Message Transport Protocol.	
39	TP++ Transport Protocol.	
40	IL Transport Protocol.	
41	IPv6 over IPv4.	RFC 2473
42	SDRP, Source Demand Routing Protocol.	
43	IPv6 Routing header.	
44	IPv6 Fragment header.	
45	IDRP, Inter-Domain Routing Protocol.	
46	RSVP, Reservation Protocol.	
47	GRE, General Routing Encapsulation.	
48	DSR, Dynamic Source Routing Protocol.	
49	BNA.	
50	ESP, Encapsulating Security Payload.	
51	AH, Authentication Header.	
52	I-NLSP, Integrated Net Layer Security TUBA.	
53	SWIPE, IP with Encryption.	
54	NARP, NBMA Address Resolution Protocol.	
55	Minimal Encapsulation Protocol.	
56	TLSP, Transport Layer Security Protocol using Kryptonet key management.	
57	SKIP.	
58	ICMPv6, Internet Control Message Protocol for IPv6. MLD, Multicast Listener Discovery.	
59	IPv6 No Next Header.	
60	IPv6 Destination Options.	
61	Any host internal protocol.	
62	CFTP.	
63	Any local network.	
64	SATNET and Backroom EXPAK.	
65	Kryptolan.	
66	MIT Remote Virtual Disk Protocol.	
67	Internet Pluribus Packet Core.	
68	Any distributed file system.	
69	SATNET Monitoring.	

70	VISA Protocol.	
71	Internet Packet Core Utility.	
72	Computer Protocol Network Executive.	
73	Computer Protocol Heart Beat.	
74	Wang Span Network.	
75	Packet Video Protocol.	
76	Backroom SATNET Monitoring.	
77	SUN ND PROTOCOL-Temporary.	
78	WIDEBAND Monitoring.	
79	WIDEBAND EXPAK.	
80	ISO-IP.	
81	VMTP, Versatile Message Transaction Protocol.	
82	SECURE-VMTP	
83	VINES.	
84	TTP.	
85	NSFNET-IGP.	
86	Dissimilar Gateway Protocol.	
87	TCF.	
88	EIGRP.	
89	OSPF, Open Shortest Path First Routing Protocol. MOSPF, Multicast Open Shortest Path First.	
90	Sprite RPC Protocol.	
91	Locus Address Resolution Protocol.	
92	MTP, Multicast Transport Protocol.	
93	AX.25.	
94	IP-within-IP Encapsulation Protocol.	
95	Mobile Internetworking Control Protocol.	
96	Semaphore Communications Sec. Pro.	
97	EtherIP.	
98	Encapsulation Header.	
99	Any private encryption scheme.	
100	GMTP.	
101	IFMP, Ipsilon Flow Management Protocol.	
102	PNNI over IP.	
103	PIM, Protocol Independent Multicast.	
104	ARIS.	
105	SCPS.	
106	QNX.	

107	Active Networks.	
108	IPPCP, IP Payload Compression Protocol.	RFC 2393
109	SNP, Sitara Networks Protocol.	
110	Compaq Peer Protocol.	
111	IPX in IP.	
112	VRRP, Virtual Router Redundancy Protocol.	RFC 3768, RFC 5798
113	PGM, Pragmatic General Multicast.	
114	any 0-hop protocol.	
115	L2TP, Level 2 Tunneling Protocol.	RFC 3931
116	DDX, D-II Data Exchange.	
117	IATP, Interactive Agent Transfer Protocol.	
118	ST, Schedule Transfer.	
119	SRP, SpectraLink Radio Protocol.	
120	UTI.	
121	SMP, Simple Message Protocol.	
122	SM.	
123	PTP, Performance Transparency Protocol.	
124	ISIS over IPv4.	
125	FIRE.	
126	CRTP, Combat Radio Transport Protocol.	
127	CRUDP, Combat Radio User Datagram.	
128	SSCOPMCE.	
129	IPLT.	
130	SPS, Secure Packet Shield.	
131	PIPE, Private IP Encapsulation within IP.	
132	SCTP, Stream Control Transmission Protocol.	
133	Fibre Channel.	RFC 6172
134	RSVP-E2E-IGNORE.	RFC 3175
135	Mobility Header.	RFC 3775
136	UDP-Lite, Lightweight User Datagram Protocol.	RFC 3828
137	MPLS in IP.	RFC 4023
138	MANET protocols.	RFC 5498
139	HIP, Host Identity Protocol.	RFC 5201
140	Shim6, Level 3 Multihoming Shim Protocol for IPv6.	RFC 5533
141	WESP, Wrapped Encapsulating Security Payload.	RFC 5840
142	ROHC, RObust Header Compression.	RFC 5858

143 - 252		
253 254	Experimentation and testing.	
255	reserved.	

This Page Intentionally* Left *Blank

IPv4 Address

- الـ IP Address هو عنوان الجهاز علي الشبكة اللي هو متوصل بيها – لازم كل جهاز يكون ليه IP علشان يقدر يتواصل مع اي جهاز تاني علشان دا العنوان بتاعه – بيتكتب بلغة الـ Decimal " 0 to 9 "
- الـ IP Address بيتكتب علي شكل 4 مقاطع – المقطع الواحد بيسمي Octet وبيفصل بين كل Octet والتاني بـ '.'

100.90.55.10

- الـ IP Address كما ذكرنا في الـ Header ان العرض بتاعه 32 Bit وبتكون من 4 Octet يعني دا معناه ان الـ Octet الواحد بيتكون من 8 Bit
- يعني اي رقم بتكتب في اي Octet بيتمثل بـ 8 Bit – اللي هي لغة الـ Binary ودي اللغة اللي بيفهمها الـ Machine

<u>طب ازاي الرقم الـ Decimal بتحول لـ Binary ؟؟</u>

- احنا عندنا الـ Bit الواحده ليها احتمالين يا إما 0 يا أما 1 - فدايما الأساس بتاعنا هو إحتمالين يعني 2 – وهما 8 Bit

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	**64**	**32**	**16**	**8**	**4**	**2**	**1**

- يعني احنا كدا عندنا لو جمعنا كل قيم الـ 2 هتدينا 255 ودا اقصي رقم ممكن اكتبه في الـ Octet وأقل رقم هو 0

✓ في طرق كتير للتحويل – بس انا بستخدم طريقة *الطرح* زي ما هوضحها كالأتي :-

<u>لو قولنا عايزين نحول رقم زي 100 مثلا :-</u>

هل الـ 100 اكبر ولا اصغر من 128 ؟ اصغر منها وبتالي مش هستخدمها , نشوف 64 هنلاقيها اكبر منها هنطرحهم من بعض الناتج هيكون 36 وبكدا استخدمنا الBit دي

نشوف اللي بعدها هل 36 اكبر من 32 ؟ اها اكبر هنطرحهم من بعض والناتج هيكون 4 وهتلاقي ان الباقي كله مش هسيتخدم الا رقم 4 فقط

ودا الناتج الإجمالي 100 → 01100100

<u>نشوف مثلا رقم زي 211</u>

نشوفهم Bit by Bit زي الطريقة اللي فاتت بالضبط

اكبر من الرقم هنستخدم الـ Bit بتاعته لو اقل مش هستخدمها وهحط مكانها 0

211 اكبر من 128 فهنستخدمها ونشوف الباقي كام ؟ الباقي 83 هنشوف اللي بعده اللي هو 64 اكبر منها فهنستخدمها وبالتالي الناتج بينهم هيكون 19 , هنشوف اللي بعده اكبر فمش هنستخدمه , نشوف الـ 16 هنلاقيها اصغر هنستخدمه والناتج هيكون 3 ودي مجموع 2 +1

ودا الناتج الإجمالي 211 → 11010011

طيب نشوف العكس كدا لو معانا رقم زي دا وعايزين نجيب الـ Decimal بتاعه :-

10101100 علشان نحسبها بشوف قيم الـ 1 كام وبجمعهم مع بعض وبالتالي دا بيكون الرقم يعني 128 + 32 + 8 + 4 = 172

- الـ IP Address المسؤول عنه هو منظمه الـ IANA " Internet Assigned Numbers Authority " :-
قولنا ان الـ IP ككل عبارة عن 32 Bit وان الـ Bit الواحدة ليها احتمالين – فعلشان نحسب عدد الـ IP's كلهم هنقول انه 2^{32}

هنلاقي الناتج بتاعها 4.292.967.296

العدد دا رغم ضخامته الا انه قليل جدا مقارنة بعدد الـ Laptops – Smart Phones – Machines – Online Sites الأجهزه دي كلها بتاخد IP's وبالتالي العدد دا صعب اوي انه يغطيهم

- فمنظمة الـ IANA حاولت تتعامل مع الموضوع دا وقسمت الـ IP لحاجه اسمها Classes وحددت لكل Class بداية ونهاية في عدد الـ IP's , اول Octet هو اللي بيحدد نوع الـ Class بتاعته

Class A	**1 – 126**
Class B	**128 – 191**
Class C	**192 – 223**
Class D	**224 - 239**
Class E	**240 – 254**

- <u>هنلاحظ ان في 3 ارقام لم يتم ذكرهم ؟</u>
- الـ 0 ودا بيكون بمثابة الـ Default Network ودا مينفعش جهاز ياخده
- الـ 127 مخصص للـ Loopback Interface اللي هو الـ NIC لو عايز تعمل عليه Test وتشوف هل هو شغال ولا فيه مشاكل . في حالة لو عندك اي مشكله في الـ Internet Connection
- الـ 255 ودا بيستخدم مع الـ Broadcasting
- Class D :- بيستخدم مع الـ Multicast اللي بتستخدم كمثال بين الـ Routing Protocols
- Class E :- مع الـ New Technology and Experiments

بعد كدا عملت حاجه اسمها الـ Subnet Mask ودي ليها استخدامين :-

1- بتحدد عنوان الشبكه اللي انا شغال عليها Network ID , Subnet
2- بتحدد عدد الأجهزه في كل شبكه

• **Class A**	**255.0.0.0**
• Class B	**255.255.0.0**
• Class C	**255.255.255.0**

بالنسبة لـ D,E ملهمش Subnet Mask علشان مش بيستخدموا مع الأجهزة

طب دا معناه ايه برضه ؟

- علشان نحسب الـ Network ID الي هو عنوان الشبكة اللي انا شغال عليها بشوف الـ IP اللي معايا دا من انهي Class والـ Class دي اساسا ايه هيا الـ Subnet Mask بتاعتها
- بعد كدا بتحول كل منهم للـ Binary – ونعمل عملية Anding بين الـ IP and Subnet Mask علشان نجيب عنوان الشبكة
- الـ Anding اني بعمل عملية ضرب بينهم الاتنين زي ما هنشوف دلوقت في المثال دا
- دا 100.50.40.17 IP عايزين نجيب عنوان الشبكة بتاعته , الواضح من الـ IP دا من Class A يعني الـ Subnet Mask بتاعته 255.0.0.0

100.50.40.17	01100100.00110010.00101000.00010001
255.0.0.0	11111111.00000000.00000000.00000000

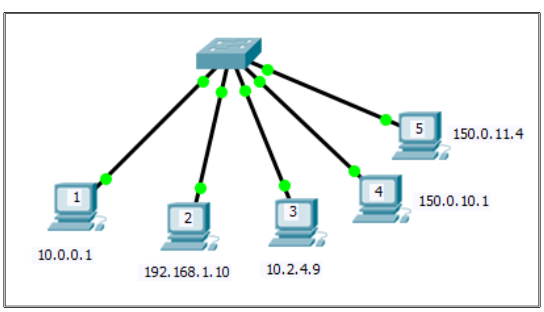
- الـ Anding الـ Bits المتشابهة بتنزل زي ما هيا , المختلفة بتنزل بـ 0

01100100.00000000.00000000.00000000

- نحوله تاني لـ Decimal هنلاقي الناتج 100.0.0.0
ودا معناه ان الـ Network ID بتاعتي هيا 100.0.0.0 يعني لازم اول Octet يكون ثابت

طيب استفدت ايه انا من الحوار دا ؟

- استفدت ان لازم الأجهزة اللي علي نفس الـ Switch تبدا كلها بأول Octet تكون قيمته 100 واي حاجة في باقي الـ Octets



لو جينا نشوف الـ Topology دي هنلاقي ان جهاز 1 مش هيعرف يتواصل مع اي جهاز متوصل معاه علي السوتش الا الجهاز رقم 3 بس علشان دا معاه في نفس الشبكة

والجهاز رقم 2 مش هيعرف يكلم اي حد اساسا عشان مفيش حد معاه واخد نفس الشبكة بتاعته

اي Network ID بيتقسم لجزئين – جزء بيسمي Network والجزء التاني بيسمي Host .

- معني كلمة Network انه لازم يكون ثابت علي كل الأجهزة اللي في شبكة واحدة علي نفس الـ Switch , اللي هو عدد الـ Bits اللي قيمتها بـ 1 في الـ Subnet Mask
- انما الـ Host بيتغير من جهاز للتاني , اللي هو عدد الـ Bits اللي قيمتها بـ 0 في الـ Subnet Mask

IP Address Classes				
Class	Format	Purpose	Address range	Max hosts
A	N.H.H.H	A few large organisations	1.0.0.0 - 126.0.0.0	16,777,214
B	N.N.H.H	Medium-size organisations	128.1.0.0 - 191.254.0.0	65,534
C	N.N.N.H	Relatively small organisations	192.0.1.0 - 223.255.254.0	254
(N = Network number, H = Host number)				

- الـ Diagram دا بيوضح كل Class فيها كام Octet للـ Network and Host وكمان بيوضح عدد الأجهزة المتاح في كل Class

Class A لازم اول Octet يكون ثابت , Class B لازم 1st Two Octets يكونوا ثابتين , Class C لازم 1st Three Octets يكونوا ثابتين في الشبكه الواحدة

- عدد الـ Zero's هو اللي بيحدد عدد الـ Hosts اللي هما عدد الأجهزة اللي هو برضه عدد الـ IP's علشان دي قيمة متغيرة

لو انا عندي شبكه فيها 50 جهاز وعايز استخدم Network معينة علي قد عدد الأجهزة اللي عندي – هل هينفع ولا لأ ؟

- لو جينا نشوف اقل شبكة ممكن تدينا IP's هنلاقي من Class C وبتدينا 256 علشان انا عندي Octet واحد بس في الـ Subnet Mask هو اللي قيمته بـ 0
- بس انا عايز 50 بس !! في الحالة دي انا بعمل حاجه اسمها Subnetting
- Subnetting يعني بقلل عدد الـ Bits بتاعه الـ Host علشان اعمل Customize لشبكة معينة تدينى احتياجاتي من الـ IP's ان انا مش عايز اشتغل بالـ Default Classes

في قانون احنا بنشتغل بيه اللي هو :- $2^h - 2 = H$

بالنسبة للـ h دي بتعبر عن عدد الـ Bits اللي هستخدمها من الـ Octets بتاعه الـ Hosts

بالنسبة للـ H بتعبر عن عدد الـ Hosts المطلوبة

ليه بنطرح 2 ؟

علشان اي شبكة احنا شغالين عليها فيها 2 IP's مش بيستخدمو اللي هما الاول والأخير

الاول بيكون اسمه الـ Network ID ودا مش بيتوزع لأي جهاز في اي شبكة , والآخير بيكون بتاع حاجه اسمها Broadcast IP

نرجع للمسألة

$2^h - 2 = 50$ $2^h = 52$

هنشوف ايه هو اقرب رقم لو بقي اوس للـ 2 هيديني الرقم اللي عايزة !! هنلاقي اقرب حاجة هو 6

يعني انا محتاج 6 Bit من الـ Host بس

الـ Hosts Bits دايما بتتحسب من جهه اليمين

11111111.11111111.11111111.11000000 دا هيكون الـ Subnet Mask بتاعها

عدد الـ Bits بتاعه الـ 1 ممكن نعبر عنهم بـ 26/

مثال

ايه هو افضل Subnet Mask لو انا عايز شبكة تديني 500 جهاز باستخدام الشبكة اللي عنوانها 10.0.0.0/8

$2^h - 2 = 500$ $2^h = 502$

هنشوف ايه هو اقرب رقم لو بقي اوس للـ 2 هيديني الرقم اللي عايزة !! هنلاقي اقرب حاجه هو 9

$2^9 = 512$

يعني انا محتاج 9 Bit من الـ Host مش الـ 24 اللي موجودين كلهم في المعطيات

هيكون الناتج هو 10.0.0.0/23 والـ Subnet Mask هنعوض عن كل قيم الـ 1 وهيكون الناتج 255.255.254.0

مثال تاني :-

لو قولنا ايه هو عدد الأجهزة المتاح في الـ Subnet Mask دا 255.240.0.0

هنشوف عندي كام Bit بتساوي 0 علشان دي بتاعه الـ Hosts وعلشان نعرفها لازم نحول الـ Subnet Mask للـ Binary

11111111.11110000.00000000.00000000 - هنلاقي عندي 20

$2^{20} - 2 = H$ H = 1.048.574

ممكن تيجي بشكل تاني اللي هو يديك الرقم علي طول بعد / يعني زي دي مثلا :-

ايه هو عدد الأجهزة وايه هو الـ Subnet Mask في الشبكة دي 21/ ؟؟

لو عندنا مثلا سؤال

بيقول ايه هي الـ Network ID الخاص بالـ IP دا – 170.55.99.17/20 ؟

كما ذكرنا علشان نحسب الـ Network ID بنقوم بعمل عملية Anding بين الـ IP and Subnet Mask .

هنا انا عندي 20/ يعني دا معناه ان عندي 20 Bit قيميتهم بـ 1

فانا ممكن محولش اول اتنين Octet علشان هما كدا كدا هيحصل ليهم Anding مع الـ 1 وهينزلو زي ما هما

170.55.99.17 → 170.55.01100011.00010001

255.255.240.0 → 255.255.11110000.00000000

هنلاقي الناتج اللي هيطلع من عملية الـ Anding هو دا :- 170.55.01100000.00000000

اللي هو 170.55.48.0/20

زي ما قولنا ان الـ Subnetting بيقلل عدد الـ Bits بتاعة الـ Host , كمان بيقسم الشبكة بتاعتي لأكتر من شبكة صغيرة وكل شبكة بيكون فيها عدد أجهزه معين " محدد "

مثال تاني :-

لو انا عايز اجيب الشبكة التالتة من الـ IP دا – 192.168.10.13/29

اول حاجة بنعملها اننا هنجيب الـ Network ID الأول زي المثال السابق :

192.169.10.00001101

255.255.255.11111000

هنلاقي الناتج بتاع الـ Anding هيكون – 192.168.8.0/29

طيب ايه بقي حكاية الشبكة التالتة ؟ لو جينا نشوف الـ Subnetting اصلا وظيفته انه بيقلل عدد الأجهزة وبيقسم الشبكة بتاعتي علشان اعرف عدد الأجهزة او ايه هو المقدار اللي هزود علي اساسه بحسب عدد الـ Bits بتاعه الHost قد ايه وبيكون دا عددهم في الشبكة دي بس , واي زيادة هتكون في شبكة تانيه

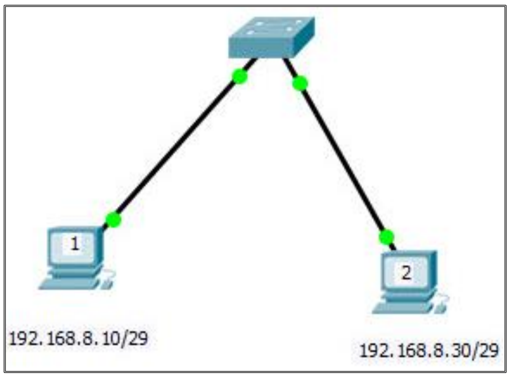
علشان اجيب الشبكه التالته – بروح علي الـ Octet الـ Mix بين الـ 1 and 0 واشوف ايه هي اقل قيمه للـ 1 في الـ Subnet Mask

255.255.255.11111000 – اقل قيمة هنا هنلاقي انها بـ 8 والـ Octet دا بيكون اسمه الـ Interest Octet

ازاي يعني ؟ طب تعالي نحسبها بالقانون اللي كنا شغالين بيه في الأول اللي هو $H = 2^h - 2$

احنا عندنا 3 Bit بتوع الـ Host وهنلاقي ان الناتج بتاعها انه هيديني 6 Valid IP انما عدد الـ IP's الإجمالي 8 . في Two IP's بيتم طرحهم اللي هما الـ Network ID & Broadcast IP

الشبكة الأولي هتكون 192.168.8.0/29 والشبكة التانيه هنزود 8 في آخر Octet علشان دا اللي فيه الـ Mix في الـ Subnet Mask فهتبقي 192.168.8.8/29 والشبكة التالته هتكون 192.168.8.16/29



لو بصينا علي الديزاين اللي قدامنا دا

هنلاقي ان PC1 مش هيعرف يعمل اي Connection مع PC2
لأن كل واحد منهم في شبكة مختلفة

اللي حدد دا هو الـ Subnet Mask بتاع كل جهاز

Subnet =Network ID

مثال تاني :-

ممكن يقولك انا عايز الشبكة الخامسة من الـ IP دا – 100.60.45.10/18 ؟

اول حاجة بنعملها اننا هنجيب الـ Network ID الأول زي المثال السابق :

100.60.45.10 → 100.60.00101101.00001010

Subnet Mask → 255.255.11000000.00000000

بعد الـ Anding هنلاقي الناتج اللي طلع :- 100.60.0.0/18

طيب ايه بقي حكاية الشبكة الخامسة ؟ لو جينا نشوف الـ Subnetting اصلا وظيفته انه بيقلل عدد الأجهزة وبيقسم الشبكة بتاعتي علشان اعرف عدد الأجهزة او ايه هو المقدار اللي هزود علي اساسه بحسب عدد الـ Bits بتاعه الHost قد ايه وبيكون دا عددهم في الشبكة دي بس , واي زيادة هتكون في شبكة تانيه

علشان اجيب الشبكة الخامسة – بروح علي الـ Octet الـ Mix بين الـ 1 and 0 واشوف ايه هي اقل قيمة للـ 1 في الـ Subnet Mask

255.255.11000000.00000000 – اقل قيمة هنا هنلاقي انها بـ 64 والـ Octet دا بيكون اسمه الـ Interest Octet

يعني انا عندي الشبكة الأولي هتكون 100.60.0.0/18 – والشبكة التانيه هزود 64 في الـ Octet بتاعها ,

وهفضل ازود لحد ما اوصل للشبكة الخامسة

طيب خلينا ناخد مثال كدا يجمع الليلة دى كلها :-

ايه هو عدد الأجهزة والـ Subnet Mask وعنوان الشبكة - والشبكة رقم خمسة - واول IP - واخر IP متاحين فيها من 192.168.50.33/27 ؟

What is the Network ID and Number of Valid Hosts and 5^{th} Network and 1^{st} IP in it ?

نجيبها وحدة وحدة كدا :-

192.168.50.00100001

Subnet Mask → 255.255.255.223 → 255.255.255.11100000

Network ID → 192.168.50.00100000 → 192.168.50.32

عدد الأجهزة المتاحة في كل شبكة اللي هو عدد الـ Bits اللي بتساوي 0 وبنحسبها من القانون :-

$2^{h} - 2 = H$ $2^{5} - 2 = H$ $H = 30$

Valid Hosts = 30 IP

طيب علشان نجيب الشبكة الخامسه – هنشوف قيمة الـ Interest Octet بكام ونزودها علي الـ ID اللي معانا

القيمة بتاعه ال1 في الـ Subnet Mask بتساوي 32 ودي اللي هنزودها

هنلاقي ان الشبكة التانيه 192.168.50.64/27 والتالته 192.168.50.96/27 والرابعه 192.168.50.128/27 ونيجي للخامسة اللي هي مطلوبة 192.168.50.160/27

اول IP متاح في الشبكه دي هو 192.168.50.161/27 علشان الـ Network ID مش بيتوزع اساسا هو مجرد عنوان للشبكه ومينفعش الأجهزة تاخده

آخر IP متاح ؟ علشان نحسبه لازم الاول نجيب الشبكة اللي بعدها 192.168.50.192/27

علشان نحسب اخر IP بنطرح 1 وبيكون الناتج هو 192.168.50.191/27 بس دا اللي هو الـ Broadcast علشان نجيب الـ Last Valid بنطرح 1 كمان وبيكون الناتج هو 192.168.50.190/27

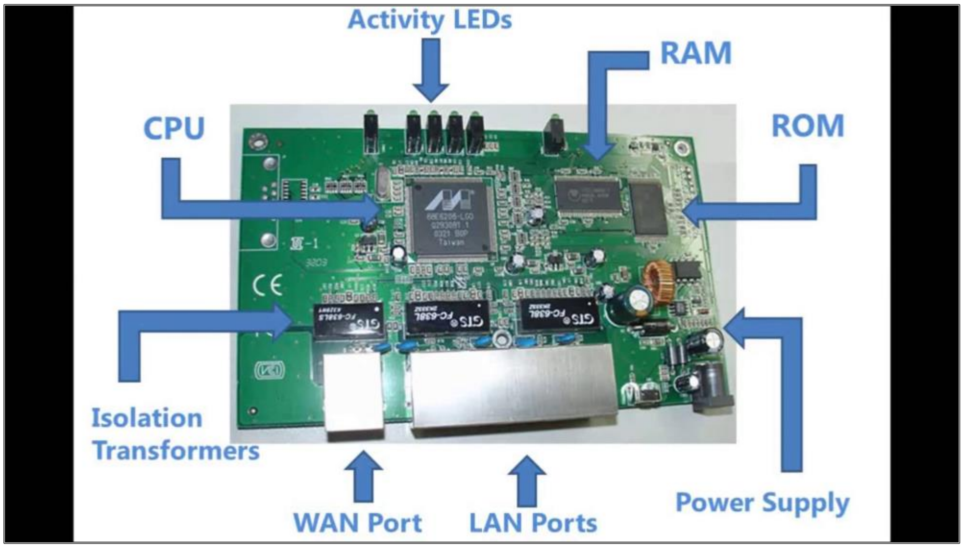
او ممكن تزود 30 مره واحده اللي هي عدد الأجهزة المتاح في كل شبكة

في المثال دا : ممكن يقولك انا عايز الشبكة الخامسة من الـ IP دا – 100.60.45.10/18 ؟

جرب كدا تحسب ايه هو اول IP وآخر IP في الشبكة الخامسه ؟؟

This Page Intentionally* Left *Blank

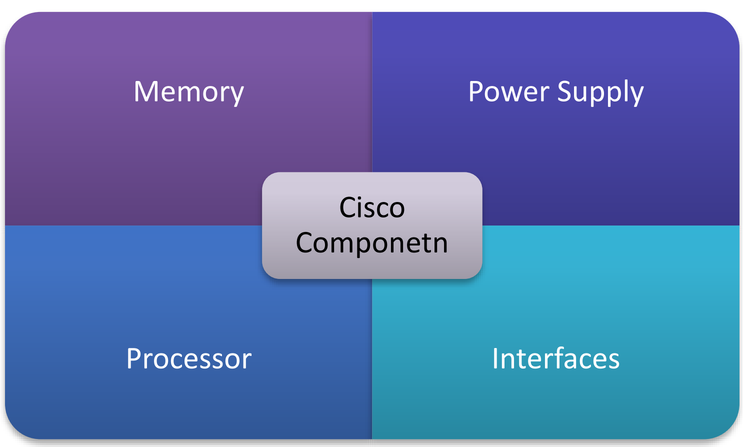
Cisco Router and Switch Component



الشابتر دا هيتكلم علي الأجهزة اللي احنا ممكن نعمل ليها Configuration لـ Service اللي احنا عايزينها مش الأجهزة اللي موجودة عندنا في البيت

في فرق كبير جدا بين الـ Switches اللي بنشتريها علشان نعمل LAN داخلية في البيت وبين الأجهزة اللي Cisco or Juniper بتقدمهم

الكلام اللي هيتقال دلوقت في الشابتر دا علي الأجهزه اللي بتقدمها Cisco



1- **Power Supply :-**

دا بيكون المسؤول عن تزويد كل الـ Component بالـ Power اللازم علشان يشتغلوا ويديونا الـ Performance اللي احنا عايزينه

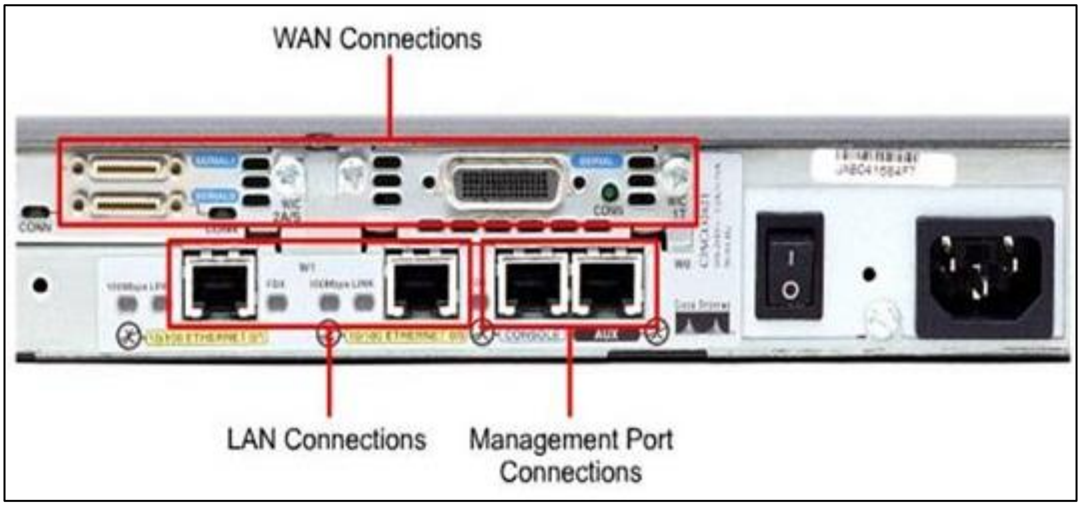
بيحول من التيار المتردد بتاع البيوت لتيار ثابت علشان مفيش اي Component يتحرق لو جاله Volt زيادة

Convert from AC to DC

<u>Interfaces</u> -2

ودي بتحدد طبيعة الأجهزة اللي هتتوصل بالـ Device هل هو سوتش ولا جهاز ولا راوتر وكل Interface ليه مميزات عن التاني وتعتبر اشهر أنواع الـ Interfaces هيا

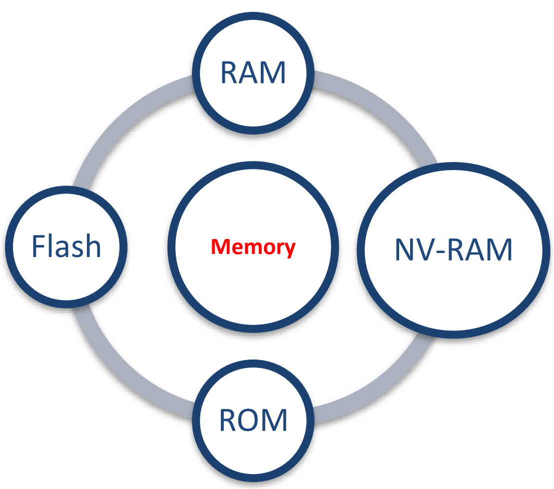
Ethernet LAN , Management Console and AUX , Serial WAN



<u>-: Processor</u> -3

مسؤول عن تنفيذ اي Configuration بنعملها علي الـ Device بيعتبر هو العقل بتاع الجهاز علشان مفيش اي حاجه بتتعمل الا ولازم يتعمل ليها Process

-: **<u>Memory</u>** -4



-: ***<u>RAM</u>***

Random Access Memory ودي بيكون فيها الـ Running Configuration يعني اي اعدادات احنا عملنا ليها تعديل او انشاء بس لسه معملناش ليها اي Save , بمجرد ما الجهاز يحصل ليه Restart هتلاقي الاعدادات دي كلها راحت

<u>-: NV-RAM</u>

دي اللي بيتحفظ فيها الإعدادات اللي انا عملتها علي الـ Device بتاعي – بيكون اسمها Saved Configuration علشان تبدأ تشتغل اول ما الجهاز يعمل Reload او يتقفل وبتفتح تاني
الـ NV-RAM بيحصل فيها Save للـ configuration الخاصه بالراوتر – انما الSwitch مفيش فيه NV-RAM فبالتالي الاعدادات بتتخزن في الـ Flash

-: Flash

دا المكان اللي بيكون عليه الـ Operating System بتاع الـ Router or Switch وبيكون اسمه IOS " Internetwork Operation System " – الإصدار الحالي منه 15.3

ROM

Read Only Memory ودي بيكون فيها الإعداد الأولية بتاعه الجهاز

	ROM - Component	Responsible for :-
1	POST	Power on Self-Test دي مسؤولة عن ان اول ما الـ Device بشتغل يعمل Check علي كل الـ Interfaces وكل الـ LED's اللي موجودة هل واخده Configuration ولا لأ و هل معمول ليها Shutdown ولا لأ علشان لو في اي Error في اي LED نقدر نعرفه
2	Boot Strap	ليها وظيفة مهمة اوي – ان اول ما الـ Device بشتغل بتروح علي الـ Flash وتجيب منه الـ IOS بتاع الـ Device . وتروح علي الـ NV-RAM وبتجيب الـ Saved Configuration وتعمل ليهم Compile مع بعض وتوديهم للـ RAM علشان يحصل ليهم Running مع بعض وبالتالي الـ Device بشتغل بالإعدادات بتاعته
3	Rommon – RX-Boot	دي بيكون فيها حاجة اسمها Configuration Register اللي هي بتحدد طبيعة الـ Booting بتاعة الـ Device نفسه وبيكون فيها الـ Basic Configuration بتاعة الـ Device .

This Page Intentionally* Left *Blank

Network Cables

الـ Cables اللي هي الأسلاك اللي بتوصل بين الأجهزة وبعض وبتقال عليها مصطلح Medium يعني وسيط بين جهازين .

ليها كذا نوع وكل نوع ليه استخدامات معينة :-

- Co-Axil Cable
- Twisted Pair
- Phone Cable
- Fiber Cable
- Console Cable

1- **Phone Cable :-**

دا الـ Cable اللي بيستخدم مع التليفون الأرضي – واللي بتيجي من خلاله خدمة الانترنت زي ما وضحنا في الشرح بتاع الـ DSLAM

ودا بيتوصل مع التليفون الأرضي عن طريق حاجه اسمها RJ-11



2- **Console Cable :-**

دا اللي بيستخدم مع Cisco Devices علشان اعمل Initial Configuration او في حالة لو عايز اعمل Password Recovery



3- Co-Axil Cable:-

دا كان اول نوع من الـ Cables كان بيستخدم في الـ Network علشان كان رخيص وكان ممكن يتوصل لمسافات كبيرة اوي وكانت الأجهزة اول ما اتصنعت كانت بتدعم النوع دا .

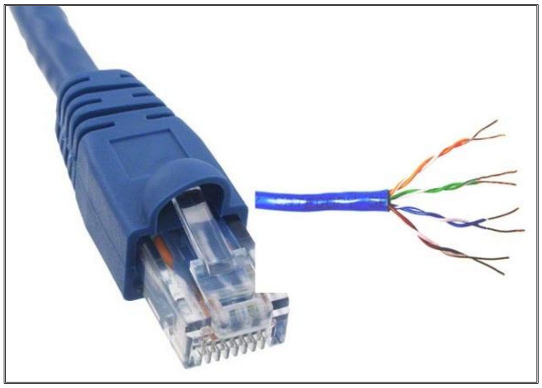
The Bandwidth for Co-Axial Cable is 10 Mbps - Megabits per second



هو شبيه للـ TV Cables اللي بنستخدمه في البيت

ليه نوعين :-

Thin (Thinnet) Cable	- Flexible coaxial cable about ¼ inch thick. - Thinnet is used for short-distance. - Thinnet connects directly to a workstation's network adapter card using a British Naval Connector (BNC). - The maximum length of thinnet is 185 meters - RG-58 family
Thick (Thicknet) Cable	- Thicknet coaxial is thicker cable than thinnet. - Thicknet cable is about ½ inch thick and can support data transfer over longer distances than thinnet. - Thicknet has a maximum cable length of 500 meters and usually is used as a backbone to connect several smaller thinnet-based networks.



4- <u>Twisted Pair :-</u>

ودا الـ Cable اللي بيتوصل بين الأجهزة حاليا – اكثر الانواع انتشارا واكثرهم استخداما في الـ LAN

Twisted يعني زوجين من الـ Cables علشان يتجنب الـ Noising and Losing للداتا اللي ممكن تحصل في عملية نقل الداتا

الاسلاك الواضحة في الصورة بيكون اسمها Pin – وبتتكون من الياف نحاسية

الـ Twisted Pair ليه نوعين :-

STP "Shielded Twisted Pair" UTP "Unshielded Twisted Pair"

الفرق بين الاتنين في نوع النحاس المستخدم والطبقة العازلة اللي بتكون موجودة بين الغلاف والـ Pin والسعر .

الـ STP بيعتبر اغلي من الـ UTP علشان النحاس بتاعه بتكون الخامة بتاعته افضل من الـ UDP

1. STP cables are shielded while UTP cables are unshielded
2. STP cables are more immune to interference and noise than UTP cables
3. STP cables are better at maximizing bandwidth compared to UTP cables
4. STP cables cost more per meter compared to UTP cables
5. STP cables are heavier per meter compared to UTP cables
6. UTP cables are more prevalent in SOHO networks while STP is used in more high-end applications

الكابلات بيتم توصيلها في الـ Data Center في حاجة اسمها Patch Panel ودي بتكون حلقه الوصل ما بين السوتشات والـ End Devices

وبيتم ترقيمها علي حسب مكان الـ Node المتصلة بكل End Device – وطبعا لازم يكون ترتيب الألوان ثابت ما بين الاتنين دول علشان ميحصلش أي مشكلة





Twisted Pair Cables Categories

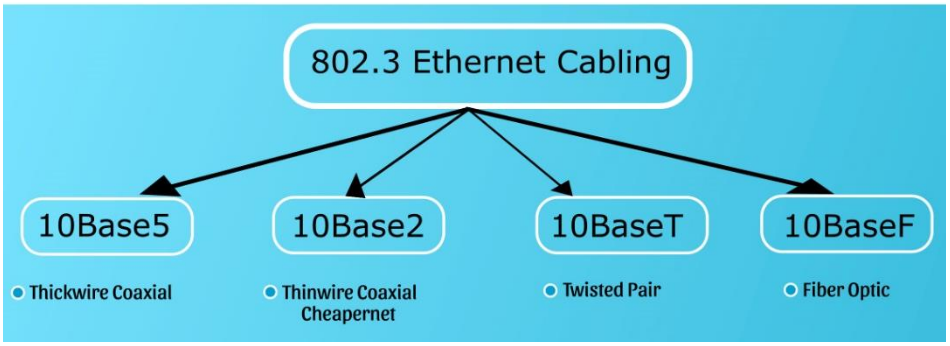
UTP Categories - Copper Cable

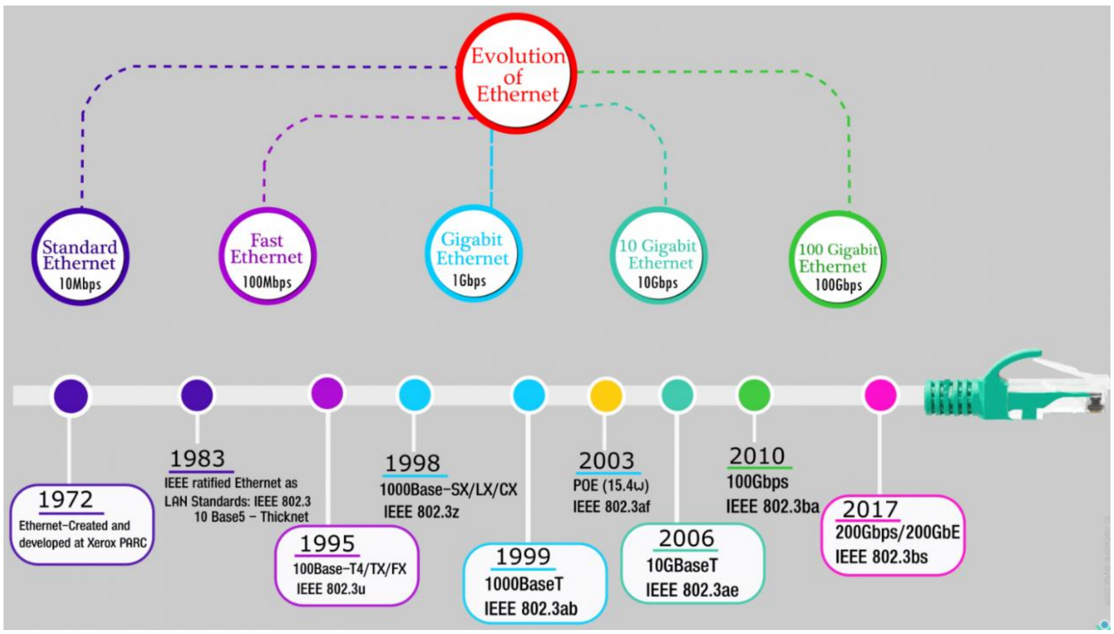
UTP Category	Data Rate	Max. Length	Cable Type	Application
CAT1	Up to 1Mbps	-	Twisted Pair	Old Telephone Cable
CAT2	Up to 4Mbps	-	Twisted Pair	Token Ring Networks
CAT3	Up to 10Mbps	100m	Twisted Pair	Token Rink & 10BASE-T Ethernet
CAT4	Up to 16Mbps	100m	Twisted Pair	Token Ring Networks
CAT5	Up to 100Mbps	100m	Twisted Pair	Ethernet, FastEthernet, Token Ring
CAT5e	Up to 1 Gbps	100m	Twisted Pair	Ethernet, FastEthernet, Gigabit Ethernet
CAT6	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT6a	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT7	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (100 meters)

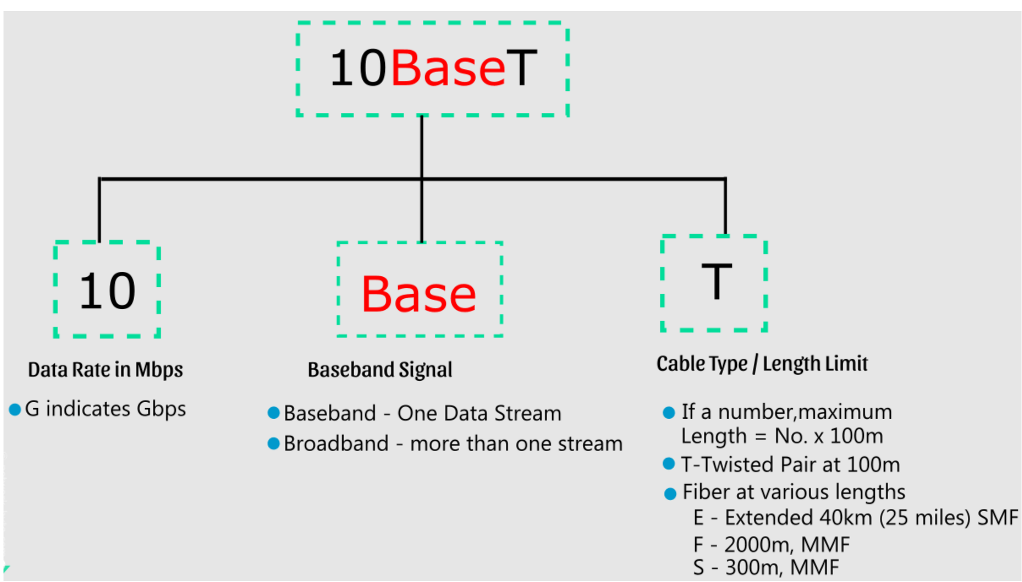
Comparison Table of LAN, Category Copper Cable

<table>
<tr><th>Items</th><th>Application</th><th>Recognised by EIA/TIA568.2-D</th><th>Networks Supported</th><th>Max. Bandwidth</th><th>Transmission Speed</th><th>Transmission Distance</th></tr>
<tr><td>Cat 5e</td><td>Residential, small office</td><td>Yes</td><td>1000BASE-T</td><td>100 MHz</td><td>1 Gbps</td><td>up to 100 meter</td></tr>
<tr><td rowspan="2">Cat 6</td><td rowspan="2">School campus and large businesses</td><td rowspan="2">Yes</td><td rowspan="2">1000BASE-TX</td><td rowspan="2">250 MHz</td><td>10 Gbps</td><td>up to 55 meter</td></tr>
<tr><td>1 Gbps</td><td>up to 100 meter</td></tr>
<tr><td>Cat 6a</td><td>Industrial, Commercial, Data Centers</td><td>Yes</td><td>10GBASE</td><td>500 MHz</td><td>10 Gbps</td><td>up to 100 meter</td></tr>
<tr><td>Cat 7</td><td>Data Centers, EMI protection</td><td>No</td><td>10GBASE</td><td>600 MHz</td><td>10 Gbps</td><td>up to 100 meter</td></tr>
<tr><td>Cat 7a</td><td>Data Centers, EMI protection</td><td>No</td><td>10GBASE</td><td>1000 MHz</td><td>10 Gbps</td><td>up to 100 meter</td></tr>
<tr><td rowspan="2">Cat 8</td><td>Industrial, Commercial, Data Centers</td><td>Yes (8.1)</td><td rowspan="2">25GBASE / 40GBASE</td><td rowspan="2">2000 MHz</td><td rowspan="2">25Gbps / 40Gbps</td><td rowspan="2">up to 30m for 25GBASE/40G BASE</td></tr>
<tr><td>Data Centers, EMI protection</td><td>No (8.2)</td></tr>
</table>

Cables Standard







On a 10BaseT network, one pair of wires in the UTP cable is used for transmission, while the second pair of wires is used for reception.
10BaseT network use two pairs of wire for full-duplex transmission. A 10BaseT network requires CAT3 or higher UTP.

100BaseT

The LAN that can use the same infrastructure as the popular 10BaseT Technology is met by 100BaseT, also known as **Fast Ethernet.** The 100BaseT is specified by the 802.3standards Which enable LANs to run at a 100Mbps data transfer rate.100BaseT uses baseband transmission and star topology as 10BaseT. The node on a 100BaseT network is configured in a star topology and the length between an end node and the hub cannot exceed 100 meters.

100BaseTX

100BaseTx is the variations of 100BaseT specified by the Institute of Electrical and Electronics Engineers (IEEE). It carries 100Mbps and used baseband signaling with a maximum distance of 100 meters per cable. It requires CAT 5 or higher unshielded twisted-pair cabling and uses the same two pairs of wire for transmission and receiving data that 10BaseT uses. Therefore, 100BaseTX is also capable of full-duplex transmission like 10BaseT.

100BaseT4

This variation of 100BaseT uses all four pairs of wires in a UTP cable and therefore, can use lower-cost CAT 3 wiring. It achieves its speed by breaking the 100Mbps data stream into three streams of 33Mbps each. These three streams are sent over three pairs of wire in the cable.

10BaseFL

10BaseFL Ethernet cable is made up of thin glass filaments. These thin glass filaments support in transmitting the light waves which carry very large amounts of data for very long distance. A fiber network is best for conditions where EMI/RFI interference is heavy. The Speed of the network is 10Mbps.The 10BaseFL network has a star Topology.62.5-micron duplex multimode fiber cable is recommended.

100BaseFX

100baseFx is a fast Ethernet network that provides 100Mbps of speed. It uses Multimode Fiber-optic (MMF) cable for transmission. The Segment Length for a half-duplex connection is 412 meters and the full-duplex connection is 2000 meters. The 100BaseFx uses the star Topology for the network connection.

1000BaseT

1000BaseT specifies Gigabit Ethernet over Cat 5e UTP cabling and provides a data transfer rate of 1000Mbps. It utilizes all four pairs of cable wires for transmission. The maximum cable segment length is 100 meters.1000BaseTx specifies Gigabit Ethernet over Car 6 cabling but is not part of the IEEE 802.3ab standard.

1000Base-CX

1000BaseCX specifies Gigabit Ethernet over a special 150-Ohm shielded coaxial cable, also known as Twinax, with DB-9 connectors. It specifically designed for short cable runs such as server-to-server connections and specifies a maximum cable length of 25 meters.

1000Base-SX

1000BaseSX is a fiber Gigabit Ethernet standard. It operates over multi-mode fiber using an 850-nanometer wavelength. This Wavelength in the light waves is near the infrared light. According to the specification given by the standards; the distance capability between the fiber endpoints of 220 m over 62.5/125 µm fiber. Although in practice, 1000BaseSX will usually work over a significantly longer distance.

Modern 50/125 µm fiber can reliably extend the signal to 500m or more. This standard is highly popular for intra building links in large office buildings, Ancillary facilities, and carrier-neutral Internet exchanges.

1000Base-Lx

1000Base-Lx is a fiber is a fiber optic gigabit Ethernet Standard, which is in long wavelength laser. The signaling speed is around 1.25±100 ppm GBd, wavelength 1270 to 1355nm.Alng with RMS spectral width maximum is 4nm typically, GbE laser will be specified as having a 1300 or 1310nm wavelength. 100Base-Lx is specified to work over a distance of up to 2km over 9µm single-mode fiber. Practically it operates well for a much greater distance. Many manufacturers will guarantee operation up to 10 or 20 Km, only if their equipment is used at both ends of the link.1000Base-Lx can also run over multi-mode fiber with a maximum segment length of 550m.

10GBase-SR

The 10Gigabit Ethernet is used for media format. These media types are designed for short wavelength(850nm). The multimode fiber (MMF) is the material used for transmission. The design goal of these media types is from 2 meters to 300 meters of fiber distance. This depends on the type and quality of the multimode fiber. The longer distance is possible depending on the qualities of the fiber optic cable used. The 10GBase-SR media type is designed for use over dark fiber, meaning a fiber cable that is not used and that is not connected to any other equipment's.

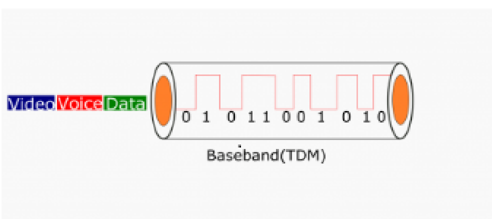
10GBase-LR

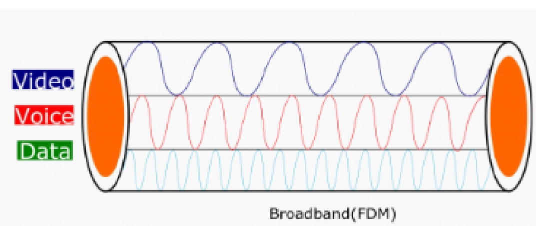
The 10GBase-LR is used for media format. These media format types are designed for use over long-wavelength (1310 nm) single-mode fiber (SMF). The design goal of these media is from 2 meters to 10 kilometers (32,808 feet) of fiber distance. It also depends on cable type and quality. The 10GBase-LR is media type that can be used over dark fiber.

10GBase-ER

The 10GBase-ER is applied for media formats. These media types are designed for use over extra-long wavelength (1550 nm) single-mode fiber (SMF). The design goal of these media types is from 2 meters up to 40 kilometers (131,233 feet), depending on cable type and quality. The 10Gbase –LR is a media type that can be used over dark fiber.

BASEBAND SIGNALING	BROADBAND SIGNALING
Baseband uses Digital signals	Broadband uses Analog Signal
Work well with Bus topology	Work well with Bus and Tree topology
Baseband communication is Bidirectional	Broadband transmission is unidirectional
Signal can be travel over Short distance	Signals can be travel over Long distance Without attenuations.
Entire bandwidth of the cable is consumed by a signal	Signals are sent on multiple frequencies, allowing multiple signals or be sent simultaneously
Baseband uses Time-Division Multiplexing	Broadband uses Frequency-Division Multiplexing(FDM)
10BaseT,10BaseF	10Broad36-Coaxial
Signaling: Manchester Encoding	Signaling: Differential PSK



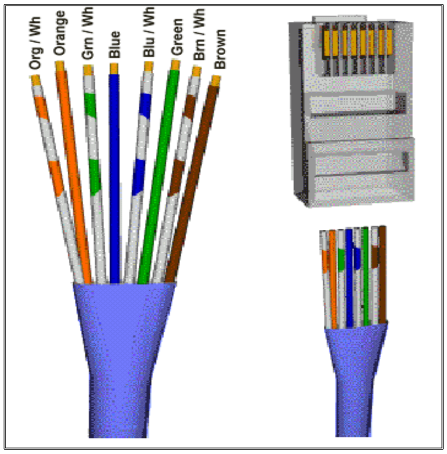


<u>Twisted-Pair Cabling Considerations</u>

- Use twisted-pair cable if:
  - Your LAN is under budget constraints.
  - You want a relatively easy installation in which computer connections are simple.
- Do not use twisted-pair cable if:
  - Your LAN requires a high level of security and you must be absolutely sure of data integrity.
  - You must transmit data over long distances at high speeds

الـ Twisted Pair Cables بتتوصل في حاجة اسمها RJ-45 ودا بيكون المكان اللي بتتحط فيه الـ Pins بتاعة الـ Cables

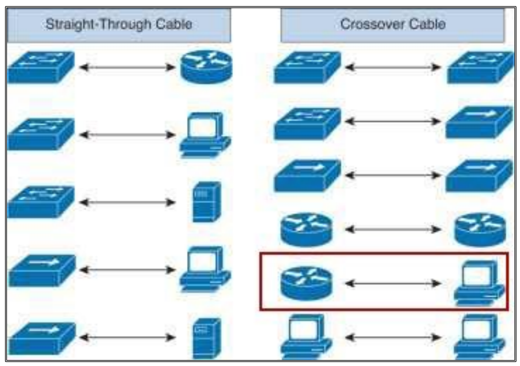




-: UTP Pins Colors

ترتيب الألوان بتاعه الـ Cables بتختلف علي حسب طبيعة التوصيل , هل الأجهزة اللي هتتوصل مع بعض دي أجهزة متشابهة ولا أجهزة مختلفة
ترتيب الألوان دا معناه اني بعمل حاجة اسمها " تأريج " يعني بحط الـ Pins في الـ RJ وبستخدم الـ Crumble اللي هيا الآراجه عشان اعمل تأريج

في نوعين من التوصيل بين الأجهزة , واللي بيحددهم هو طبيعة ترتيب الألوان في الـ RJ :-
Straight Through- ودا بيستخدم للتوصيل مع الأجهزة المختلفه يعني جهاز مع سوتش او سوتش مع راوتر
Cross Over – ودا بيستخدم للتوصيل مع الأجهزة المتشابهة



القاعدة الشاذة الوحيدة في التوصيل هي بين جهاز وراوتر علي الرغم من انهم اجهزة مختلفة الا ان نوع الـ Cable اللي بيستخدم بيكون Cross Over

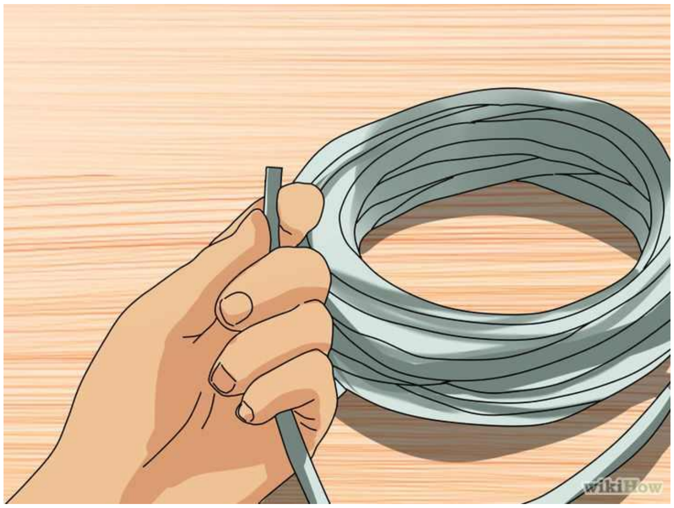
1	White and Orange
2	Orange
3	White and Green
4	Blue
5	White and Blue
6	Green
7	White and Brown
8	Brown

دا بيكون الترتيب بتاع طرف من الطرفين بتوع الـ Cable والطرف التاني علي حسب الـ Device المتصل بيه اي بمعني تاني علي حسب طريقة التوصيل , هل هي Straight Through ولا Cross Over

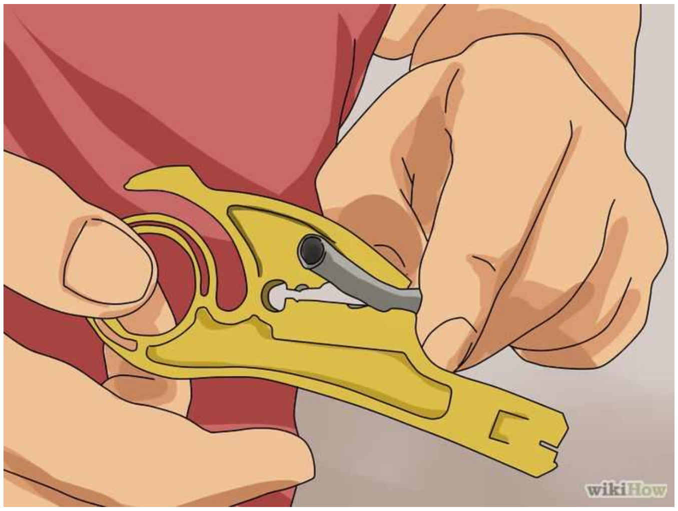
لو الطرف التاني كان زي الطرف الأول يبقي كدا التوصيل نوعه Straight Through
لو عملنا تبديل للـ Pin 1 with 3 and 2 with 4 يبقي كدا الـ Cable دا هيتوصل Cross Over

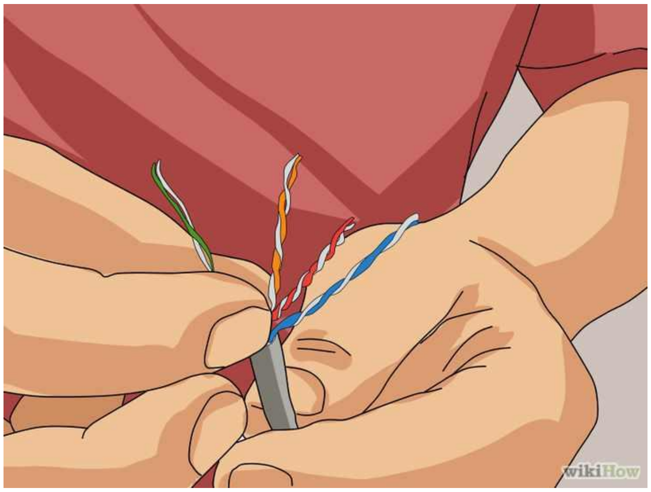
مش كل الـ Pin 8 بيستخدموا في نقل الداتا – الـ Pins الأساسية هي 1,2,3,6 والباقي بيستخدم مع تكنولوجي POE " Power Over Ethernet "

How to Make a Network Cable

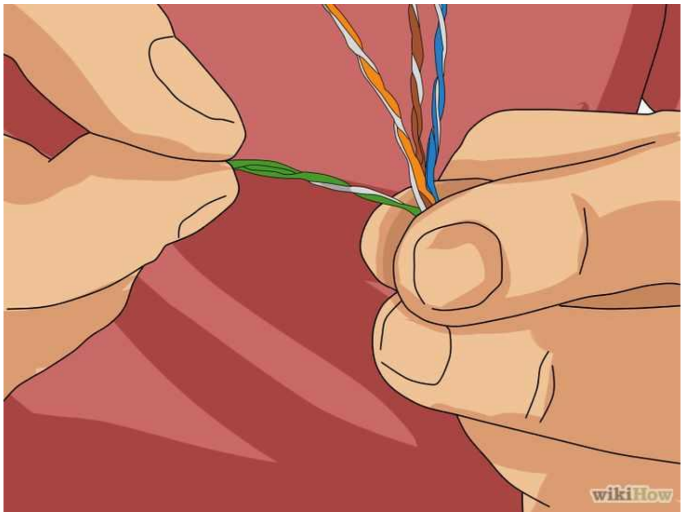


بنعمل عملية تقشير للـ Cable علشان نشيل الطبقة العازلة اللي عليه

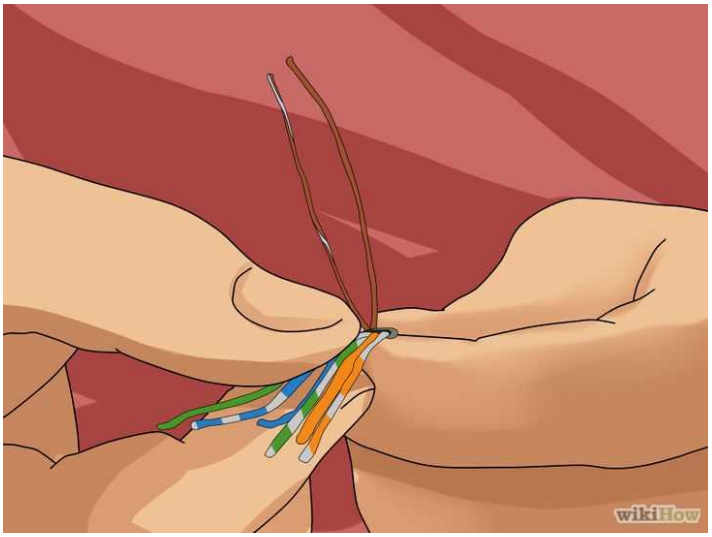




بنفرد كل Pair من بعضه



وبنبدأ نخليهم علي استقامة واحدة



ونشوف ترتيب الألوان اللي هنستخدمه ايه هو ؟

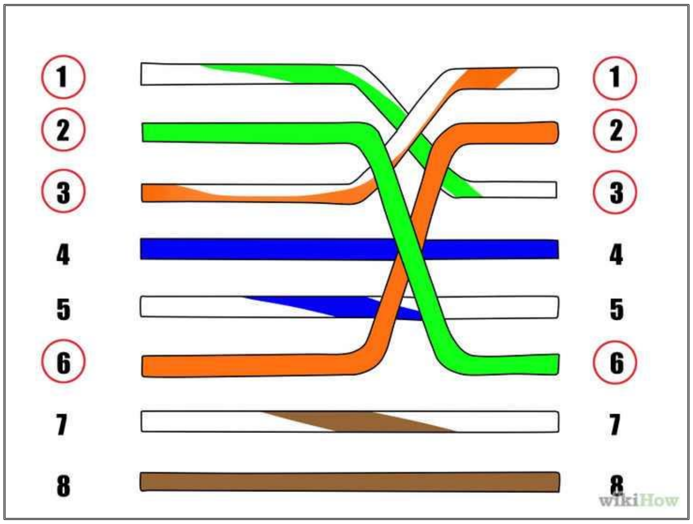
568B - Put the wires in the following order, from left to right:

- white orange
- orange
- white green
- blue
- white blue
- green
- white brown
- brown

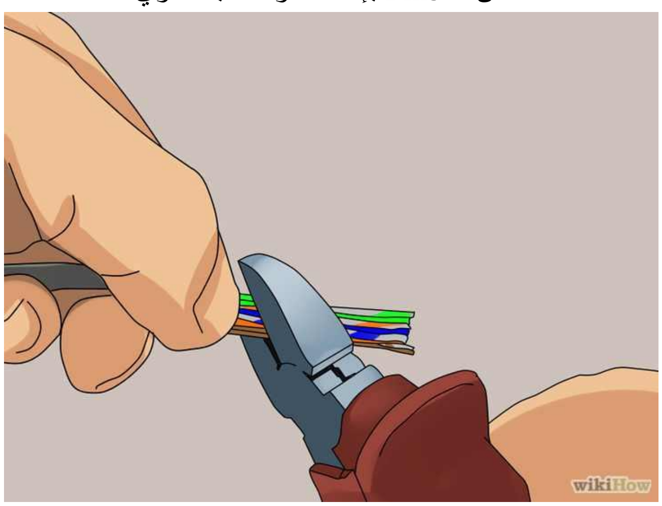
568A - from left to right:

- white/green

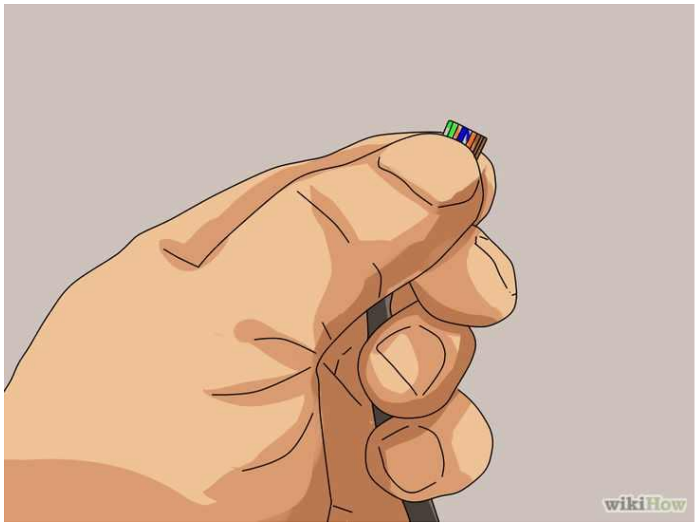
- green
- white/orange
- blue
- white/blue
- orange
- white/brown
- brown



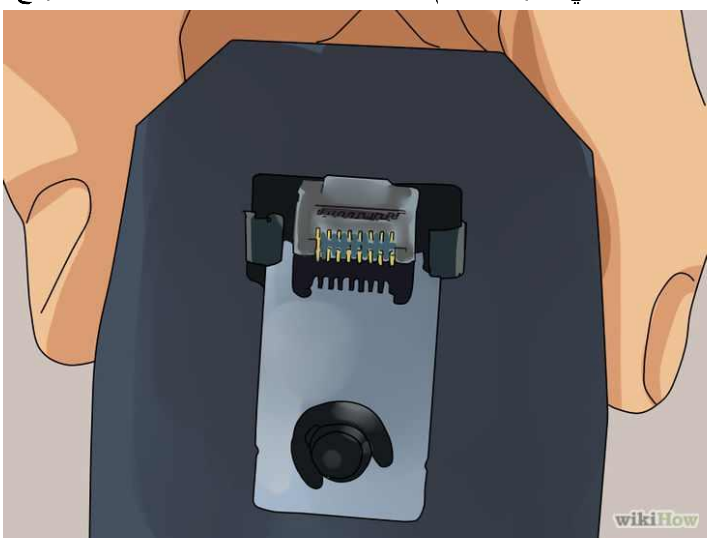
نقص الـ Pins بإستقامة واحدة بالتساوي



ودا بيكون الشكل اللي المفروض يظهر قدامك



بعد كدا بيجي دور استخدام الـ Crumble علشان نعمل عملية التأريج



بعد كدا بتعمل Test للـ Cable دا علشان تشوف عملية التأريج كانت ناجحة ولا لأ

